Data protection

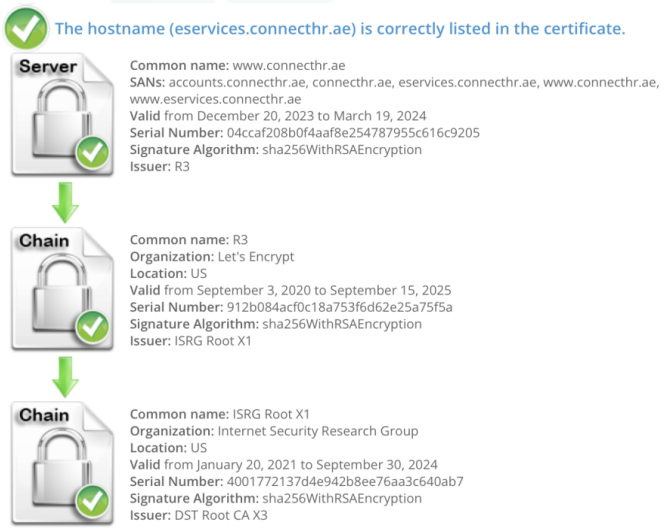
How is sensitive data (including client data) protected?

The protection of sensitive data, including client data, is a critical aspect of information security. Organizations implement various measures to ensure the confidentiality, integrity, and availability of sensitive information. Here are some common practices and technologies used to protect sensitive data:

Encryption:

Data in Transit: Encrypting data while it's being transmitted over networks helps prevent unauthorized access during the transfer. Secure protocols such as HTTPS (SSL/TLS) are commonly used for web traffic.

Data at Rest: Encrypting data when it is stored on servers, databases, or other storage devices adds an additional layer of protection. Full disk encryption and database encryption are examples of this approach.



Access Controls:

Implement strict access controls to ensure that only authorized individuals have access to sensitive data. Role-based access control (RBAC) and least privilege principles are commonly used to limit access to the minimum necessary for job functions.

Authentication & Authorization:

Use strong authentication mechanisms, such as multi-factor authentication (MFA), to verify the identity of users. Authorization ensures that users can only access data and perform actions that are within their defined scope of responsibilities.

Data Masking and Redaction:

Implement techniques like data masking and redaction to conceal sensitive information in non-production environments or when displaying data to users who don't need to see the complete dataset.

Regular Auditing and Monitoring:

Employ logging and monitoring systems to track access to sensitive data. Regularly review logs and audit trails to detect and respond to any suspicious or unauthorized activities.

Data Backups:

Regularly back up sensitive data to ensure its availability in case of accidental deletion, data corruption, or other unforeseen incidents. Backup systems should also be secured to prevent unauthorized access.

Endpoint Security:

Implement security measures on endpoint devices, such as computers and mobile devices, to protect against malware, unauthorized access, and data breaches. This includes antivirus software, firewalls, and device encryption.

Security Training and Awareness:

Educate employees and stakeholders about security best practices, social engineering threats, and the importance of safeguarding sensitive information. Human error is a common factor in data breaches, and awareness training can help mitigate risks.

Incident Response Plan:

Develop and regularly update an incident response plan to address security incidents promptly. This includes a defined process for reporting and responding to data breaches.

Compliance with Regulations:

Adhere to relevant data protection regulations and industry standards. Compliance with regulations such as GDPR, HIPAA, or PCI DSS helps ensure that organizations handle sensitive data responsibly and ethically.

By combining these measures, organizations can create a comprehensive security posture to protect sensitive data and maintain the trust of their clients and stakeholders. Keep in mind that the specific measures adopted may vary depending on the nature of the data, industry regulations, and organizational requirements.

Customer data is segregated.

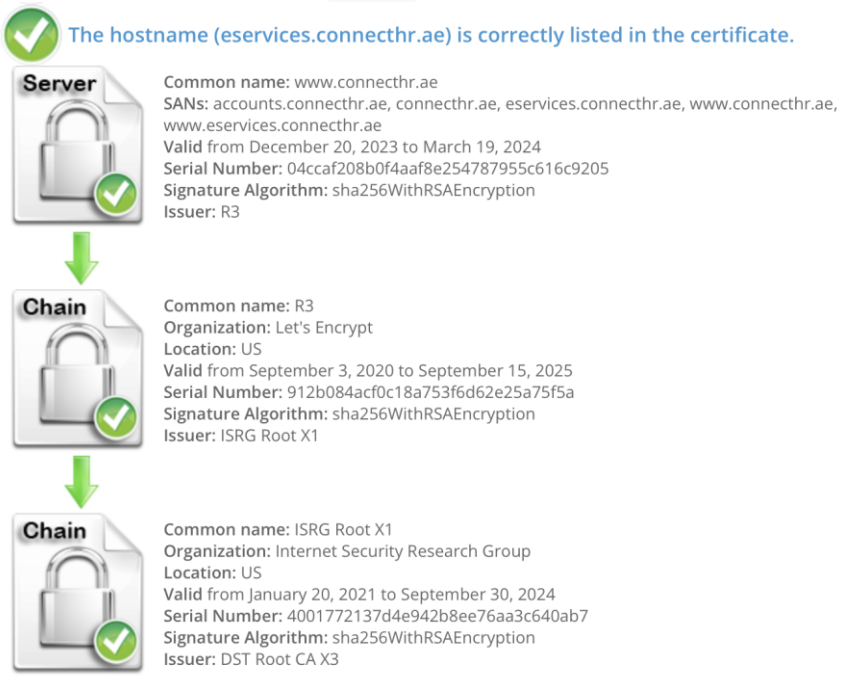
Connect HR stores client's data in an independent database which means that data is not stored with other client's data.

Other information like documents or images are stored in an independent folder and restricted for users.

Sensitive data is encrypted at rest.

Sensitive data is encrypted in transit.

Data transmitted from client side to server is encrypted with certificate SHA256



Detail of SSL Certificate configured on connecthr.ae
Source: https://www.sslshopper.com/ssl-checker.html#hostname=connecthr.ae

Question: How are backups performed?

Security control:

- **Backup information is logged.**
- **Backup restoration tests or integrity tests are performed periodically.**
- **Data backups for important business information are carried out periodically.**

Connect HR Answer: The process of backing up data within our organization incorporates a crucial security control: the logging of backup information. This control is instrumental in providing visibility into the backup activities, ensuring accountability, and facilitating effective monitoring and auditing.

To adhere to this security control, detailed logs are generated for each backup operation. These logs include comprehensive information such as the date and time of the backup, the source and destination of the backup, the specific files or data sets included, and any relevant status or error messages.

The technical implementation involves leveraging backup software and systems that are configured to generate these logs automatically. This ensures consistency and accuracy in capturing essential details of each backup activity.

Additionally, log retention policies are in place to guarantee that the necessary information is retained for an appropriate duration, aligning with regulatory requirements and organizational policies.

Regular reviews and audits of backup logs are conducted to validate the effectiveness of the logging process. These assessments involve confirming that all relevant backup events are captured, analyzing logs for any anomalies or potential issues, and ensuring that the logged information aligns with the backup policies in place.

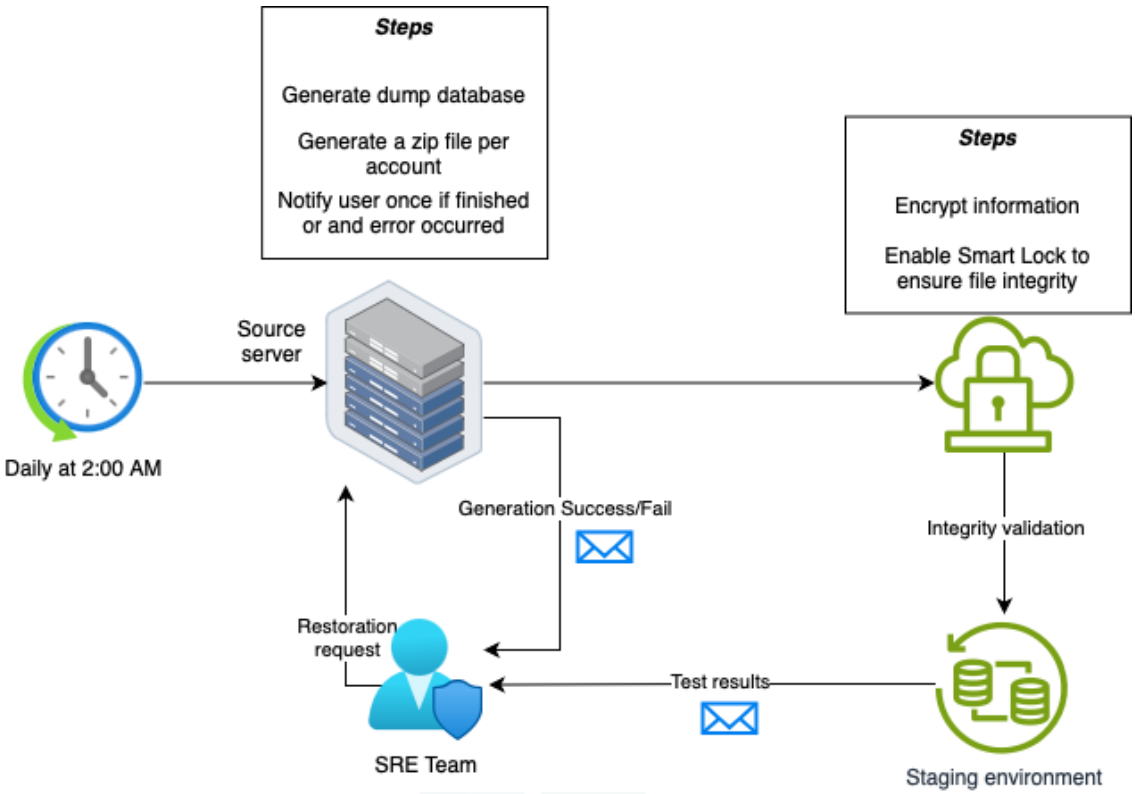
Moreover, the backup log information serves as a critical component of our incident response and recovery strategies. In the event of data loss or system failure, these logs play a pivotal role in tracing the history of backup activities, expediting the identification of issues, and facilitating the restoration process.

In summary, our organization diligently adheres to the security control of logging backup information, leveraging automated processes and regular audits to ensure the completeness and accuracy of backup logs. This practice enhances accountability, supports effective monitoring, and contributes to the overall resilience of our data backup procedures.

Data backups for important business information are carried out periodically.

Automated job runs daily to create a copy of the application in a zip format with documents and images uploaded. To the application.

Database information is exported in SQL format.Once both files are created it keeps on the server while a copy is transferred to another location.



Backup restoration tests or integrity tests are performed periodically.

Once in a month a backup is restored in the local machine to validate the integrity of the information.

How are business continuity plans managed?

A business impact analysis (BIA) is conducted

Business Impact Analysis

1. Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the *Connect HR.* It was prepared on January 13 2024

.

1.1 Purpose

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.

The BIA is composed of the following three steps:

Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.

Identify resource requirements. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

Identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the *Connect HR* Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system, including, but not limited to, the Disaster Recovery Plan (DRP) or Cyber Incident Response Plan.

2. System Description

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including inputs and outputs and telecommunications connections.

Note: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan.

3. BIA Data Collection

Data collection can be accomplished through individual/group interviews, workshops, email, questionnaires, or any combination of these.

3.1 Determine Process and System Criticality

Step one of the BIA process - Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

Mission/Business Process	Description
Payroll generation	*Process to generate monthly employee payroll, uses all information stored on the application to generate reports*
Employee attendance	Register shift employee of daily attendance
Employee onboarding/offboarding	Manage the process to onboarding and offboarding employees
Document generation	Helps on the generation of document for employees with financial, insurance or laboral information

If criticality of mission/business processes has not been determined outside of the BIA, the following subsections will help to determine criticality of mission/business processes that depend on or support the information system.

3.1.1 Identify Outage Impacts and Estimated Downtime

This section identifies and characterizes the types of impact categories that a system disruption is likely to create in addition to those identified by the FIPS 199 impact level, as well as the estimated downtime that the organization can tolerate for a given process. Impact categories should be created and values assigned to these categories in order to measure the level or type of impact a disruption may cause. An example of cost as an impact category is provided. Organizations could consider other categories like harm to individuals and ability to perform mission. The template should be revised to reflect what is appropriate for the organization.

Outage Impacts

Impact categories and values should be created in order to characterize levels of severity to the organization that would result for that particular impact category if the mission/business process could not be performed. These impact categories and values are samples and should be revised to reflect what is appropriate for the organization.

The following impact categories represent important areas for consideration in the event of a disruption or impact.

Impact values for assessing category impact:

- Severe = 3-4
- Moderate = 2
- Minimal = 1

The table below summarizes the impact on each mission/business process if *Connect HR* were unavailable, based on the following criteria:

Mission/Business Process	Impact Category				
	Financial	Operational	Employee Productivity	Information Security	Impact
Payroll generation	x	x	x		Severe
Employee attendance		x	x		Moderate
Employee onboarding/offboarding		x	x	x	Severe
Document generation				x	Minimal

Estimated Downtime

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration as a result of a disruptive event.

Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on *Connect HR*. *Values for MTDs and RPOs are expected to be specific time frames, identified in hourly increments (i.e., 8 hours, 36 hours, 97 hours, etc.).*

Mission/Business Process	MTD	RTO	RPO
Payroll generation	*48 hours*	*48 hours*	*24 hours (last backup)*
Employee attendance	6 hours	12 hours	24 hours (last backups)
Employee onboarding/offboarding	24 hours	48 hours	24 hours (last backup)
Document generation	72 hours	48 hours	24 hours

Include a description of the drivers for the MTD, RTO, and RPOs listed in the table above (e.g., mandate, workload, performance measure, etc.).
Include a description of any alternate means (secondary processing or manual work-around) for recovering the mission/business process(es) that rely on the system. If none exist, so state.

Question: How do you ensure the proper and effective implementation of cryptographic controls to protect your data?

Security control: The rules for the management of encryption keys are formalized and implemented.

Connect HR Answer:

The proper and effective implementation of cryptographic controls to protect our data is a top priority within our organization. A crucial aspect of this effort is the formalization and implementation of rules for the management of encryption keys.

To ensure robust key management, we have defined and documented clear rules governing the entire lifecycle of encryption keys. This includes key generation, distribution, storage, usage, rotation, and eventual disposal. The rules are established based on industry best practices and compliance standards, such as NIST SP 800-57, to ensure a secure and standardized approach to key management.

The technical implementation of these rules involves the use of a centralized key management system. This system not only generates and distributes cryptographic keys securely but also enforces policies for their proper usage. Access controls are implemented to restrict key management privileges to authorized personnel only.

Regular audits and assessments are conducted to validate the adherence to key management rules. These assessments include reviewing key management policies, auditing key usage logs, and validating that key rotations and updates are performed according to the defined rules. Any deviations or anomalies are promptly addressed through corrective actions.

In addition, personnel involved in key management undergo comprehensive training to ensure awareness and understanding of the established rules. This includes proper procedures for key handling, secure storage, and adherence to key management policies.

To further enhance security, cryptographic modules and algorithms used for key management are selected based on recognized standards and undergo regular security assessments. This ensures that the cryptographic controls implemented in our organization meet industry benchmarks for confidentiality and integrity.

In summary, our organization places a strong emphasis on the proper and effective implementation of cryptographic controls, specifically in the area of key management. The formalized rules, technical safeguards, regular audits, and personnel training collectively contribute to a secure and resilient cryptographic infrastructure, safeguarding our data from unauthorized access and ensuring the confidentiality of sensitive information.

Question: How do you ensure the proper and effective implementation of cryptographic controls to protect your data?

Security control: The encryption keys are logically separated from encrypted data.

Connect HR Answer:

Ensuring the proper and effective implementation of cryptographic controls is a priority within our organization, with a focus on the security control of maintaining logical separation between encryption keys and encrypted data.

To achieve this, we employ dedicated key management systems that securely generate, store, and distribute encryption keys independently of the encrypted data. This separation is a deliberate design choice to minimize the risk of unauthorized access to both the keys and the encrypted information.

Cryptographic modules, including Hardware Security Modules (HSMs), play a pivotal role in enforcing this separation. HSMs provide a secure environment for key operations, ensuring that keys are processed in isolation from the systems hosting the encrypted data. This adds an additional layer of protection, requiring potential attackers to overcome a secure enclave to gain access to the keys.

Ongoing access controls are enforced within the key management systems to restrict access to authorized personnel. Regular training programs emphasize the importance of maintaining this logical separation, guiding personnel on secure key handling practices and emphasizing the security benefits of this approach.

Periodic assessments validate the effectiveness of the logical separation, including reviews of access logs and verification that cryptographic modules operate securely. These assessments contribute to continuous improvement, ensuring that the separation of keys from encrypted data remains a resilient security control.

In summary, our organization is committed to the logical separation of encryption keys from encrypted data, utilizing dedicated key management systems and cryptographic modules. This approach enhances the security of our cryptographic infrastructure, minimizing the risk of unauthorized access to sensitive information.

Question: How is safe user navigation and browsing ensured?

Security control: Downloading of executable or risky files is blocked.

Connect HR Answer:

Ensuring safe user navigation and browsing within Google Workspace is a paramount concern for our organization, and a crucial security control in this context is the proactive blocking of downloads for executable and risky files.

To enforce this security control, we leverage the security features inherent in Google Workspace. Specifically, we utilize Google Drive's built-in security settings and policies to restrict the upload and sharing of executable files and files associated with known risks.

Google Workspace's integrated security controls include advanced threat detection mechanisms, which actively scan files during upload and download processes. Any attempt to download files with executable extensions or those identified as risky triggers immediate intervention, preventing the download and mitigating potential threats.

Periodic reviews and assessments of security logs within Google Workspace provide tangible evidence of instances where downloads of executable or risky files were successfully blocked. This continuous monitoring ensures the ongoing effectiveness of our restrictions and allows for prompt adjustments in response to emerging threats.

In addition to technological controls, user education and awareness are integral components of our strategy. Through training programs and communication, we inform users about the risks associated with downloading certain file types and emphasize the importance of compliance with our security policies within Google Workspace.

In summary, our organization has implemented robust measures within Google Workspace to block the download of executable and risky files. Leveraging the native security features, regular monitoring, and user education contribute to maintaining a secure environment for user navigation and browsing within the Google Workspace ecosystem.

Question: How does the company ensure that electronic messaging (email) infrastructure, and its usage, are safe?

Security control: Email is secured against malware.

Connect HR Answer:

Ensuring the safety of our electronic messaging infrastructure, particularly within Google Workspace/Gmail, is a top priority for our organization. A crucial security control in this context is the implementation of measures to secure email against malware.

To achieve this, we utilize the robust security features embedded within Google Workspace/Gmail. Specifically, we employ the built-in anti-malware solutions that automatically scan incoming and outgoing emails for malicious content. These solutions employ advanced threat detection mechanisms to identify and neutralize malware, including viruses, ransomware, and other malicious attachments or links.

The effectiveness of our anti-malware measures is evident through regular monitoring and analysis of security logs within Google Workspace. These logs provide tangible evidence of instances where the anti-malware solution successfully intercepted and mitigated potential threats within email communications.

Continuous updates to threat intelligence feeds are integrated into Google Workspace/Gmail's security infrastructure. This ensures that our anti-malware solutions remain current and adaptive to emerging threats, providing a proactive defense against the evolving landscape of malicious activities.

Educational initiatives are also part of our strategy to enhance email security. Users receive training on recognizing phishing attempts, suspicious email content, and the importance of not interacting with potentially harmful emails. This user awareness contributes to a multi-layered defense against email-borne threats.

In summary, our organization ensures the safety of our electronic messaging infrastructure, particularly within Google Workspace/Gmail, by leveraging the native anti-malware solutions. Ongoing monitoring, regular updates, and user education collectively contribute to maintaining a secure email environment and protecting against potential malware threats.

Question: How is monitoring performed to detect security events?

Security control: Activity on business applications are monitored.

Connect HR Answer:
Monitoring for the detection of security events is actively performed within our organization, with a specific focus on business applications. We employ advanced monitoring tools and solutions to track and analyze activity within these applications, aiming to identify potential security incidents and anomalies.

The monitoring process includes the collection and analysis of logs generated by business applications. These logs capture user activities, system transactions, and other relevant events. Through the use of dedicated security information and event management (SIEM) systems, we correlate and analyze this data to detect patterns indicative of security threats or unauthorized access.

To ensure the effectiveness of monitoring, alerting mechanisms are configured to promptly notify security personnel of any suspicious activities. These alerts trigger an immediate response to investigate and mitigate potential security incidents.

Regular reviews of monitoring configurations and alerting thresholds are conducted to adapt to changing security requirements and to fine-tune the system for optimal performance. Additionally, the monitoring process aligns with industry standards and compliance mandates to address specific security and regulatory considerations.

In summary, our organization actively monitors the activity within business applications, utilizing advanced tools, SIEM systems, and alerting mechanisms. This approach enhances our ability to detect and respond to security events promptly, contributing to a proactive security posture.

Question: How is your network secured?

Security control: The network is segregated.

Connect HR Answer: Our network security is reinforced through the implementation of network segregation, ensuring a robust defense against potential security threats. The network is logically divided into distinct security zones, each with specific access controls and tailored security measures.

This segregation is achieved through the deployment of firewalls, routers, and access controls that restrict communication between different network segments. By enforcing these security measures, we mitigate the risk of lateral movement by potential attackers and limit the impact of security incidents.

To ensure the effectiveness of network segregation, access controls are regularly reviewed and updated. This includes validating that only necessary communication is allowed between different security zones and that any unauthorized attempts to cross security boundaries are promptly detected and blocked.

Additionally, network segmentation aligns with industry best practices and regulatory requirements, providing a defense-in-depth strategy to safeguard sensitive data and critical systems. Regular audits and assessments are conducted to verify the proper implementation and adherence to network segmentation policies.

In summary, our network security is enhanced through the deliberate segregation of the network into different security zones. This proactive approach strengthens our overall security posture, limits the potential impact of security incidents, and aligns with industry standards and regulatory expectations.

Question: How is your network secured?

Security control: Administration of the network is secured.

Connect HR Answer: Our network administration is systematically secured to mitigate potential security risks. This involves implementing several measures to safeguard the privileged access and control of network infrastructure.

Access to network administration functions is restricted to authorized personnel, and strong authentication mechanisms, such as multi-factor authentication (MFA), are enforced. This ensures that only authenticated and authorized individuals can perform administrative tasks.

Secure communication channels, such as encrypted protocols and virtual private networks (VPNs), are employed for remote administration. This helps protect sensitive information exchanged during administrative activities from potential eavesdropping or tampering.

Furthermore, access controls are configured to grant the minimum necessary privileges to network administrators. This principle of least privilege ensures that individuals have access only to the resources and commands required for their specific roles, reducing the potential impact of compromised credentials.

Regular audits and reviews of network administration logs are conducted to detect and respond to any suspicious activities. These logs capture details of administrative actions, facilitating the identification of unauthorized changes or potential security incidents.

In summary, our network administration is secured through a combination of access controls, authentication mechanisms, encrypted communication channels, and regular auditing practices. This comprehensive approach ensures the protection of network infrastructure and reduces the risk of unauthorized access or malicious activities.

Question: How are wireless networks secured?

Security control: Wireless network access is protected.

Connect HR Answer: Our wireless networks are diligently secured to safeguard against unauthorized access and potential security threats. Several measures are in place to protect wireless network access

1. Strong Encryption: We enforce the use of robust encryption protocols, such as WPA3, to encrypt data transmitted over the wireless network. This ensures that data exchanged between devices and access points is secure and cannot be easily intercepted.

2. Network Authentication: Access to the wireless network is controlled through strong authentication mechanisms, such as WPA3-Enterprise, which utilizes individual user credentials for authentication. This adds an additional layer of security, preventing unauthorized devices from connecting to the network.

3. Pre-Shared Key (PSK) Management: In cases where WPA3-Enterprise is not feasible, WPA3-Personal (PSK) is implemented with strong, regularly updated pre-shared keys. This minimizes the risk associated with static keys and unauthorized access.

4. SSID Management: The Service Set Identifier (SSID) is configured to be non-broadcast, reducing the visibility of the wireless network. This measure helps deter unauthorized users from attempting to connect.

5. Access Point Placement: Access points are strategically placed to minimize signal leakage beyond the intended coverage area. This reduces the risk of unauthorized access from neighboring locations.

6. Regular Security Audits: Our wireless network undergoes regular security audits and assessments to identify and address vulnerabilities. This includes reviewing access logs, analyzing wireless traffic patterns, and conducting penetration testing.

In summary, our wireless networks are secured through a combination of strong encryption, authentication mechanisms, SSID management, strategic access point placement, and ongoing security audits. These measures collectively contribute to a robust defense against unauthorized access and potential security risks in our wireless infrastructure.

Question: How is remote access secured?

Security control: Only approved devices are allowed to access the internal network.

Connect HR Answer: Our approach to securing remote access involves a strict control measure: only approved devices are permitted to access the internal network. This security control is crucial for preventing unauthorized personal devices from connecting remotely to the company's information systems.

To implement this control, we employ a combination of device authentication and access controls. Remote access solutions are configured to verify the identity and compliance of devices attempting to connect to the internal network. Only devices that meet predefined security standards, such as having up-to-date antivirus software and operating system patches, are granted access.

Additionally, user authentication mechanisms, including multi-factor authentication (MFA), are enforced to ensure that even approved devices can only be accessed by authorized individuals. This adds an extra layer of security by requiring users to verify their identity through multiple means, reducing the risk of unauthorized access.

Regular reviews and audits of device access logs are conducted to monitor and ensure the ongoing effectiveness of the security controls. Any attempts from unauthorized or non-compliant devices are promptly detected and addressed.

In summary, our remote access security is fortified by allowing only approved devices to connect to the internal network. This multi-layered approach, combining device authentication, access controls, and user authentication mechanisms, helps prevent unauthorized personal devices from compromising the security of our information systems.

Question: How are network flows managed?

Security control: The opening and closing of network flows are managed and reviewed.

Connect HR Answer:

The management of network flows within our organization is reinforced through a dedicated security control: the oversight of the opening and closing of network flows. To ensure the effectiveness of this control, we maintain a systematic process for managing and reviewing the initiation and termination of network flows.

Network flow management involves monitoring and controlling the communication streams between devices and systems. This includes the establishment of connections, data transfer, and the termination of these connections. To maintain a secure environment, we enforce policies that govern the proper opening and closing of network flows.

Regular reviews of network flow logs are conducted to assess the legitimacy of connection activities. This includes scrutinizing the logs for any anomalies, unauthorized connections, or patterns indicative of potential security incidents. The reviews are integral to identifying and responding promptly to any unauthorized or suspicious network flow activities.

The management of network flows aligns with industry best practices and compliance requirements. This ensures that our network operations adhere to recognized standards and that any deviations or potential security risks are promptly addressed.

In summary, our organization actively maintains and reviews the opening and closing of network flows as a fundamental security control. This proactive approach, supported by regular reviews and adherence to industry standards, contributes to the overall security and integrity of our network infrastructure.

Question: How are network flows managed?

Security control: Authentication flows are encrypted.

Connect HR Answer:

The management of network flows, with a specific focus on authentication, is reinforced through a crucial security control: the encryption of authentication flows. To ensure the implementation and effectiveness of this control, the organization actively ensures that network authentication flows are encrypted.

Authentication flows involve the exchange of sensitive information such as user credentials. To protect this information from potential eavesdropping or interception, the organization employs robust encryption protocols. This includes the use of secure cryptographic algorithms to encrypt the transmission of authentication data during the authentication process.

The technical implementation involves the deployment of encryption technologies such as HTTPS for web-based authentication flows and secure authentication protocols like EAP-TLS for network-based authentication. These measures ensure that authentication data is transmitted securely, mitigating the risk of unauthorized access or tampering during the authentication process.

To provide evidence of the encryption of authentication flows, the organization conducts regular assessments and audits. These assessments include reviews of cryptographic configurations, validation of secure transmission channels, and confirmation that encryption standards align with industry best practices. Documentation of these security measures and their effectiveness serves as tangible evidence of the organization's commitment to ensuring the encryption of authentication flows.

In summary, the organization actively ensures that network authentication flows are encrypted, employing robust encryption protocols and conducting regular assessments to verify the effectiveness of these security measures. This proactive approach safeguards sensitive authentication information and upholds the confidentiality and integrity of the authentication process within the network flows.

Question: How is the use of mobile devices managed?

Security control: A centralized management solution for mobile devices (Mobile Device Management - MDM) with access to company data is deployed.

Connect HR Answer:

The use of mobile devices within our organization is strategically managed through the deployment of a centralized Mobile Device Management (MDM) solution. This robust security control ensures secure access to company data and enhances the overall management of mobile devices.

To address this security control, we have implemented a comprehensive MDM solution that provides centralized oversight and control over mobile devices accessing company data. This includes smartphones, tablets, and other mobile devices used by employees. The MDM solution is configured to enforce security policies, device configurations, and access controls consistently across the mobile device fleet.

The MDM solution includes features such as:

1. Device Enrollment: All mobile devices accessing company data are required to be enrolled in the MDM system, ensuring visibility and control.

2. Security Policies: The MDM solution enforces security policies, such as password requirements, device encryption, and biometric authentication, to enhance the security posture of mobile devices.

3. Remote Wipe and Lock: In case of loss or theft, the MDM solution enables remote wipe and lock functionalities to protect sensitive company data from unauthorized access.

4. Application Management: The MDM solution facilitates the management of company-approved applications, ensuring a secure and controlled environment for business-related activities.

5. Compliance Monitoring: Regular monitoring of device compliance ensures that mobile devices adhere to the defined security standards and policies.

To provide evidence of the deployment of the MDM solution, we maintain documentation outlining the configuration settings, security policies, and usage reports generated by the MDM system. Regular audits and assessments are conducted to verify the proper functioning of the MDM solution and its alignment with security requirements.

In summary, our organization actively deploys and maintains a centralized Mobile Device Management (MDM) solution to manage mobile devices accessing company data. This approach

enhances security, enforces compliance, and provides a centralized platform for effective mobile device management.

Question: How is the use of mobile devices managed?

Security control: An application catalog is built to ensure that only approved applications can be installed on mobile devices.

Connect HR Answer:

The use of mobile devices within our organization is diligently managed through the implementation of a crucial security control: the establishment of an application catalog. This catalog serves as a comprehensive list of approved applications, ensuring that only authorized and secure applications can be installed on mobile devices.

To address this security control, we have defined and implemented a catalog of approved applications. This catalog outlines a curated list of applications that meet security, compatibility, and functionality criteria established by the organization. The catalog is regularly updated to include new approved applications and remove any that no longer meet the defined standards.

Key components of the application catalog management include:

1. Application Approval Process:** New applications undergo a thorough approval process before being included in the catalog. This process involves security assessments, compatibility checks, and reviews to ensure the application aligns with organizational policies.

2. Version Control: The catalog includes information about approved versions of applications. This ensures that only the authorized and up-to-date versions are installed on mobile devices, reducing the risk of vulnerabilities associated with outdated software.

3. Access Controls: Access to the application catalog is restricted to authorized personnel, and only approved administrators have the authority to modify or update the catalog. This ensures the integrity of the catalog and prevents unauthorized changes.

To provide evidence of the application catalog's effectiveness, documentation is maintained detailing the catalog's contents, the approval process for applications, and regular updates. Audits and assessments are conducted to verify compliance with the defined application catalog and ensure that only approved applications are installed on mobile devices.

In summary, our organization actively defines and maintains an application catalog to ensure that only approved applications can be installed on mobile devices. This proactive approach enhances security, reduces the risk of unauthorized or insecure applications, and contributes to the overall management of mobile device usage within the organization.

Question: How is the use of mobile devices managed?

Security control: A revocation process for mobile devices in the event of theft or loss, or when they are no longer needed, is formalized and implemented.

Connect HR Answer: In case the mobile is mandatory to advise it as soon as he is aware off. With Google Workspace we can block the entire mobile in a span of 5 minutes. https://support.google.com/a/answer/7543044?hl=en

Question: How are business applications, including applications that process client data, inventoried and classified?
Security control: The maximum admissible unavailability time for each application is defined.

Connect HR Answer:

To ensure effective management and oversight of business applications, including those processing client data, our organization follows a meticulous process of inventorying and classifying applications. This is accompanied by defining the maximum acceptable unavailability time for each application. Here's how we achieve this:

Application Inventory:

We maintain a comprehensive inventory of all business applications within our organization. This inventory includes details such as the application name, purpose, owner, criticality to business operations, and whether it processes client data.

Classification Criteria:
Applications are classified based on their criticality to business functions, the sensitivity of the data they handle (especially client data), and their overall impact on organizational operations. The classification criteria include factors like data confidentiality, integrity, and availability requirements.

Maximum Admissible Unavailability Time:
For each inventoried business application, we define the maximum admissible unavailability time. This is the predetermined acceptable duration for which an application can be offline or unavailable without significantly impacting business operations or breaching service level agreements.

Risk Assessment:
Risk assessments are conducted to identify potential vulnerabilities and threats to each business application. These assessments consider the impact of unavailability on business processes, data integrity, and client service delivery.

Stakeholder Collaboration:
Collaboration with application owners, business units, and stakeholders is integral to the classification process. Input from various stakeholders ensures that the classification aligns with business priorities and accurately reflects the importance of each application.

Documentation:
The classification details and maximum admissible unavailability time for each business application are documented and regularly updated. This documentation serves as a reference point for both technical and non-technical staff involved in application management and maintenance.

Continuous Monitoring:

Continuous monitoring is established to track the availability and performance of business applications in real-time. This enables us to proactively identify potential issues and take preventive measures to minimize unavailability.

Incident Response Planning:

In the event of unexpected application unavailability, incident response plans are in place. These plans outline the steps to be taken to restore services within the defined maximum admissible unavailability time, minimizing the impact on business operations.

Regular Review and Adjustment:

The classification and maximum admissible unavailability time for applications are subject to regular reviews. Adjustments are made based on changes in business priorities, technological advancements, and emerging threats to ensure ongoing alignment with organizational goals.

Question: How are employees made aware of and trained in information security risks?

Security control: Information security awareness is appropriate to user roles and responsibilities.

Connect HR Answer:

The awareness and training of employees in information security risks within our organization are actively managed to align with the security control of tailoring information security awareness to user roles and responsibilities.

Key Components of our Information Security Awareness Program:

1. Information security awareness training is tailored to the specific roles and responsibilities of employees within the organization. Different user groups receive targeted training relevant to their functions, ensuring that the content is meaningful and applicable to their daily tasks.

2. Training materials are customized to address business needs and industry-specific risks. This includes scenarios, examples, and case studies that resonate with the organization's context, making the training more relevant and engaging for employees.

3. Information security training is regularly updated to reflect evolving threats, technologies, and organizational policies. This ensures that employees receive the most current and applicable information to enhance their awareness of potential security risks.

4. Interactive Training Formats: Training sessions incorporate interactive formats, such as simulations, quizzes, and workshops, to engage employees actively. This approach enhances the effectiveness of the training by encouraging participation and knowledge retention.

5. Communication Channels: Information security awareness is promoted through various communication channels, including emails, newsletters, and internal communications. This reinforces key messages and keeps employees informed about the latest security developments.

***Evidence of Compliance:**

Documentation includes records of role-based training plans, customized training content, and regular updates to training materials. Participation metrics, quiz scores, and feedback from employees are also collected and analyzed to gauge the effectiveness of the information security awareness program.

In Summary: Our organization ensures that information security awareness is not only appropriate to user roles and responsibilities but is also tailored to business needs. This approach enhances the relevance and effectiveness of our information security training, contributing to a culture of heightened awareness and proactive risk mitigation among our employees.

Question: How are employees made aware of and trained in information security risks?

Security control: Information security awareness is provided to all users.

Connect HR Answer:

Information Security Awareness Policy

1. Purpose: The purpose of this Information Security Awareness Policy is to ensure that all employees within the organization are equipped with the knowledge and understanding necessary to mitigate information security risks. This policy outlines the mandatory information security awareness training program designed to reach every user, fostering a culture of shared responsibility and proactive risk mitigation.

2. Scope:
This policy applies to all employees within the organization, regardless of their roles or responsibilities. It encompasses both in-house and remote workers.

3. Policy Statement:
All employees must undergo information security awareness training to enhance their understanding of security risks and best practices. The training program will be comprehensive, mandatory, and regularly updated to reflect emerging threats and changes in organizational policies.

4. Key Components:4.1. Universal Training Coverage:
Information security awareness training will be designed to reach every user within the organization, ensuring that all employees receive fundamental knowledge about security risks and best practices.

4.2. Mandatory Training Sessions:
Participation in information security awareness training sessions is mandatory for all employees. This policy emphasizes the shared responsibility of maintaining a secure working environment.

4.3. Multichannel Communication:
Information security messages will be communicated through various channels, including email, intranet announcements, and awareness campaigns. This multichannel approach maximizes the reach of key security messages to all users.

4.4. Regular Training Updates: Training materials will be regularly updated to reflect emerging threats, changes in technology, and evolving organizational policies. This ensures that employees are equipped with current knowledge to address contemporary security challenges.

4.5. Interactive Learning Modules:

Training sessions will incorporate interactive elements such as simulations, quizzes, and real-world scenarios to enhance engagement, knowledge retention, and the practical application of security principles in daily tasks.

5. Evidence of Compliance:
Documentation will include records of attendance in mandatory training sessions, completion rates for online modules, and communication logs for information security awareness campaigns. Periodic assessments and quizzes will be conducted to gauge the effectiveness of the training program, with results informing continuous improvement efforts.

***6. Enforcement:** Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

7. Review and Updates: This policy will be reviewed regularly to ensure its relevance and effectiveness in addressing information security risks. Updates will be made as necessary to align with emerging threats and changes in organizational practices.

8. Approval:
This Information Security Awareness Policy is approved by Connect HR

Question: How are employees made aware of and trained in information security risks?

Security control: Social engineering awareness campaigns are carried out for all users.

Connect HR Answer:

Social Engineering Awareness Policy

1. Purpose:
The purpose of this Social Engineering Awareness Policy is to ensure that all employees within the organization are effectively trained and made aware of social engineering risks. This policy outlines the implementation of a comprehensive social engineering awareness program for all users.

2. Scope:
This policy applies to all employees within the organization, irrespective of their roles or responsibilities. It includes both in-house and remote workers.

3. Policy Statement:
All employees must undergo social engineering awareness training as part of the organization's commitment to mitigating risks associated with social engineering attacks. This policy emphasizes the importance of cultivating a vigilant and informed workforce.

4. Key Components:
4.1. Universal Training Coverage:
The social engineering awareness program will be designed to reach every user within the organization, ensuring that all employees are equipped with the knowledge to identify and respond to social engineering threats.

4.2. Mandatory Training Sessions:
Participation in social engineering awareness training sessions is mandatory for all employees. This policy underscores the shared responsibility of maintaining a secure working environment by being vigilant against social engineering tactics.

4.3. Simulated Campaigns:
Regular social engineering awareness campaigns will be conducted, including simulated phishing and other social engineering attacks. These campaigns aim to assess and enhance employees' ability to recognize and appropriately respond to such threats.

4.4. Reporting Mechanisms:
Employees will be educated on reporting mechanisms for suspected social engineering attempts. The organization encourages a culture of reporting to promptly address and analyze potential security incidents.

4.5. Continuous Education:

The social engineering awareness program will be an ongoing initiative, with regular updates and additional training sessions to address emerging threats and tactics employed by attackers.

5. Evidence of Compliance:

Documentation will include records of attendance in mandatory social engineering awareness training sessions, participation rates in simulated campaigns, and records of reported incidents. Regular assessments and evaluations will be conducted to gauge the effectiveness of the program.

6. Enforcement: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

7. Review and Updates:

This policy will be reviewed regularly to ensure its relevance and effectiveness in addressing social engineering risks. Updates will be made as necessary to align with emerging threats and changes in organizational practices.

8. Approval:

This Social Engineering Awareness Policy is approved by Connect HR

Question: How are employees made aware of and trained in information security risks?

Security control: Employees are trained in detecting suspicious behavior and alert rise.

Connect HR Answer:

Behavioral Awareness Training Policy

1. Purpose:

The purpose of this Behavioral Awareness Training Policy is to establish a framework for training all employees within the organization to effectively detect and report suspicious behavior. This policy aims to enhance the overall security posture by empowering employees to play an active role in identifying potential threats.

2. Scope:

This policy applies to all employees within the organization, regardless of their roles or responsibilities. It encompasses both in-house and remote workers.

3. Policy Statement:

All employees must undergo behavioral awareness training to develop the skills necessary for recognizing suspicious behavior and reporting it effectively. This policy emphasizes the importance of fostering a culture of vigilance and cooperation to safeguard organizational assets.

4. Key Components:

4.1. Universal Training Coverage:

The behavioral awareness training program will be designed to reach every user within the organization, ensuring that all employees possess the skills to identify and report suspicious behavior.

4.2. Mandatory Training Sessions:

Participation in behavioral awareness training sessions is mandatory for all employees. This policy underscores the shared responsibility of maintaining a secure working environment by actively contributing to the detection of potential threats.

4.3. Recognizing Suspicious Behavior:

Employees will be trained to recognize patterns of behavior that may indicate potential security threats. This includes but is not limited to unusual access attempts, unauthorized presence in restricted areas, or any behavior deviating from normal activities.

4.4. Reporting Procedures:

The training program will include clear guidance on reporting procedures for employees who observe suspicious behavior. This involves educating employees on how to promptly and accurately report their observations to the designated authorities.

4.5. Simulated Scenarios:

The training sessions may include simulated scenarios to provide practical experience in identifying and responding to suspicious behavior. These scenarios will be designed to mimic real-world situations to enhance the effectiveness of the training.

5. Evidence of Compliance:

Documentation will include records of attendance in mandatory behavioral awareness training sessions, participation rates in simulated scenarios, and records of reported incidents. Regular assessments and evaluations will be conducted to gauge the effectiveness of the program.

6. Enforcement:

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

7. Review and Updates:

This policy will be reviewed regularly to ensure its relevance and effectiveness in addressing the organization's security needs. Updates will be made as necessary to align with emerging threats and changes in organizational practices.

Question: How are Information Security roles and responsibilities managed?

Security control: The roles and responsibilities concerning information security are defined.

Connect HR Answer:

Information Security Roles and Responsibilities Policy

1. Purpose:

The purpose of this Information Security Roles and Responsibilities Policy is to establish a structured framework defining the roles and responsibilities related to information security within the organization. This policy aims to ensure clarity, accountability, and effective management of information security functions.

2. Scope:

This policy applies to all employees, contractors, and third-party entities involved in the processing or handling of organizational information. It encompasses both in-house and remote workers.

3. Policy Statement:

Roles and responsibilities concerning information security will be clearly defined and documented to establish a foundation for effective management and oversight of information security practices within the organization.

4. Key Components:

4.1. Role Definition:

Distinct roles related to information security will be identified based on job functions and responsibilities. This includes, but is not limited to, roles such as Information Security Officer, Data Custodians, System Administrators, and end-users.

4.2. Responsibilities Allocation:

Clear responsibilities will be allocated to each defined role. This will ensure that each individual or team understands their specific obligations related to information security and contributes effectively to the overall security posture.

4.3. Communication Channels:

Established communication channels will facilitate the flow of information regarding security roles and responsibilities. This includes regular updates, briefings, and documentation accessible to all relevant personnel.

4.4. Training and Awareness:

Training programs and awareness initiatives will be implemented to ensure that individuals in defined roles are equipped with the necessary knowledge and skills to fulfill their information security responsibilities effectively.

4.5. Periodic Review:

Roles and responsibilities will be subject to periodic review to align with changes in organizational structure, technology, or regulatory requirements. Updates will be made as needed to reflect evolving information security needs.

5. Evidence of Compliance:

Documentation will include a comprehensive list of defined roles and their associated responsibilities. Records of training sessions, communication logs, and periodic reviews will be maintained to provide evidence of ongoing compliance with defined roles and responsibilities.

6. Enforcement:

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

7. Review and Updates:

This policy will be reviewed regularly to ensure its relevance and effectiveness. Updates will be made as necessary to align with changes in organizational structure, technology, or regulatory requirements.

Question: How is physical access to facilities and critical areas managed?

Security control: Physical access reviews are carried out periodically.

To ensure the effective management of physical access to facilities and critical areas, our organization is committed to conducting thorough and periodic access reviews. The process is designed to enhance security, align with organizational needs, and address potential risks. Here's how we conduct these reviews:

1. Scheduling and Frequency:

We establish a clear schedule for conducting periodic access reviews. The frequency is determined based on the sensitivity of the areas, organizational changes, and regulatory requirements. This ensures that reviews are conducted regularly and in a timely manner.

2. Cross-Functional Collaboration:

Physical access reviews involve collaboration between multiple departments, including security, human resources, and facilities management. This cross-functional approach ensures that access permissions align with current roles and responsibilities across the organization.

3. Defined Access Criteria:

We establish well-defined criteria for granting and maintaining access to facilities and critical areas. This includes specifying roles that require access, business justifications, and any additional security considerations. The criteria serve as a foundation for the review process.

4. Review Teams and Responsibilities:

Dedicated review teams are assigned specific responsibilities for conducting access reviews. These teams consist of representatives from relevant departments who are knowledgeable about the access requirements of their respective areas.

5. Automated Access Review Tools:

We leverage automated tools designed for access reviews to streamline the process. These tools help identify discrepancies, anomalies, or unauthorized access quickly and efficiently. Automation enhances the accuracy and effectiveness of the reviews.

6. Risk-Based Approach:

The access review process follows a risk-based approach. Higher-risk areas undergo more frequent and detailed reviews, ensuring that areas with greater security implications receive heightened attention.

7. Employee and Manager Involvement:

Employees and their managers actively participate in the access review process. This involvement ensures that access rights are validated with current job responsibilities and that any changes are promptly communicated and addressed.

8. Documentation and Reporting:

Comprehensive documentation is maintained throughout the access review process. This includes records of individuals' access rights, review outcomes, and any corrective actions taken. Regular reports are generated to track and communicate the results of the reviews.

9. Continuous Training and Awareness:

Training programs and awareness initiatives are conducted regularly to educate employees about the importance of access reviews. This fosters a culture of security awareness and ensures that employees understand their role in maintaining the integrity of the access control system.

By implementing these measures, our organization aims to conduct periodic physical access reviews that are not only systematic and efficient but also aligned with industry best practices. This approach enhances our ability to manage access effectively, mitigate risks, and maintain a secure environment for our facilities and critical areas.

Question: How is physical access to facilities and critical areas managed?

Security control: A process for deleting physical accesses at the end of activity or when they are no longer needed is implemented.

Connect HR Answer:

Access Review Procedures:

Regularly conduct access reviews to identify individuals with physical access rights. This includes reviewing access lists, security badges, and other physical access control mechanisms.

Termination Notification Workflow:

Implement a workflow that triggers an immediate notification to the security and IT teams upon an employee's termination or change in roles. This notification should include details such as the employee's name, position, and the reason for access modification.

Collaboration with HR:
Establish a collaborative relationship with the Human Resources (HR) department. Ensure that HR promptly communicates any employee terminations or role changes to the security team to initiate the access removal process.

Access Control System Integration:
Integrate the physical access control system with HR databases to automate the access removal process. This integration ensures that access is revoked in real-time when HR updates employment statuses.

Verification Protocols:
Implement verification protocols to confirm access removal requests. This may include dual-authorization requirements or confirmation from multiple stakeholders before access is disabled.

Immediate Access Removal:
Ensure that physical access removal is immediate upon employee termination or role change, especially for sensitive areas such as server rooms. Implement procedures to deactivate access cards, update biometric systems, and revoke any electronic keys.

Documentation and Audit Trails:
Maintain detailed documentation and audit trails for all access removal activities. This documentation should include the date, time, and individuals involved in the access removal process, providing a transparent record for compliance and security audits.

Employee Exit Interviews:
Conduct exit interviews with departing employees to retrieve physical access cards and keys. Clearly communicate the importance of returning these items as part of the exit process.

Regular Training and Awareness:

Conduct regular training sessions to raise awareness among employees and security personnel about the importance of timely physical access removal. Ensure that all stakeholders understand the potential risks associated with delayed access revocation.

Periodic Access Reviews:
Implement periodic access reviews, not only for terminated employees but for all individuals with physical access rights. This ongoing process helps identify and address access rights that are no longer necessary.

Continuous Improvement:
Establish a continuous improvement feedback loop to regularly evaluate and enhance the physical access removal process. Gather feedback from security personnel, HR, and other stakeholders to identify areas for improvement.

By defining and implementing this comprehensive process, the organization can effectively manage physical access removals, mitigating the risk of unauthorized entry and ensuring the security of sensitive areas, such as server rooms, at all times.

Question: How is information security integrated into projects?

Security control: Security tests are carried out before projects are put into production.

1. Purpose:

The purpose of this Security Testing Policy is to establish guidelines and procedures to ensure that comprehensive security tests are conducted before the rollout of any project within the organization. This policy aims to identify and mitigate potential security risks, safeguard sensitive information, and uphold the overall security posture of the organization.

2. Scope:

This policy applies to all projects, including software development, system upgrades, infrastructure changes, and any other initiatives that involve the introduction or modification of information systems within the organization.

3. Policy Statement:

Security testing is a critical component of the project development lifecycle. All projects, regardless of size or complexity, must undergo thorough security testing before being approved for rollout. This includes assessments of both technical and non-technical aspects that may impact the security of the organization's information assets.

4. Key Components:

4.1. Pre-Deployment Security Assessment:

A pre-deployment security assessment must be conducted for each project. This assessment includes a review of the project's architecture, code, configurations, and dependencies to identify potential vulnerabilities.

4.2. Vulnerability Scanning:

Conduct automated vulnerability scanning to identify known vulnerabilities in software, applications, and infrastructure components. This should be performed at multiple stages of the project development lifecycle.

4.3. Penetration Testing:

Engage in penetration testing to simulate real-world attacks on the project's environment. This includes testing for weaknesses in network security, application security, and other potential entry points for malicious actors.

4.4. Code Review:

Perform a comprehensive code review to identify security vulnerabilities in the project's source code. This includes assessing coding practices, input validation, and adherence to secure coding standards.

4.5. Data Security Assessment:

Evaluate how the project handles and protects sensitive data. This includes an assessment of data encryption, storage, transmission, and disposal practices to ensure compliance with data protection regulations.

5. Responsibility:

The project team, including developers, system administrators, and project managers, is collectively responsible for ensuring that security tests are conducted. The organization's Information Security Officer (ISO) will oversee and coordinate the security testing process.

6. Testing Frequency:

Security tests must be conducted at key milestones during the project development lifecycle, including but not limited to development, staging, and pre-production phases. Additionally, periodic reviews should be conducted for ongoing projects to identify and address emerging security risks.

7. Reporting and Remediation:

A detailed report of security test findings, including vulnerabilities and recommendations, must be documented. The project team is responsible for addressing identified issues promptly. The project will not proceed to rollout until all identified security vulnerabilities are remediated and validated.

8. Exceptions:

Exceptions to this policy must be documented and approved by the organization's Information Security Officer. Any exceptions should include a risk assessment and mitigation plan.

9. Review and Updates:

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates will be made as necessary to align with changes in technology, regulations, or organizational requirements.

10. Enforcement:

Non-compliance with this policy may result in project delays, additional security assessments, or other disciplinary actions as deemed appropriate by the organization's leadership.

Question: How is sensitive data (including client data) protected?

Security control: Customer data is segregated.

Connect HR Answer:

Server Partitioning:
To demonstrate the segregation of client data on servers, the organization employs server partitioning practices. Each server is logically divided into distinct partitions, and access controls are implemented to ensure that only authorized personnel have access to specific partitions housing client data.

Documentation Example:
Extract from Server Configuration Document:
Server Name: [Server Name]
Partitions:
Partition 1: [Purpose - e.g., Web Application]
Partition 2: [Purpose - e.g., Database Storage]
Partition 3: [Purpose - e.g., Backups]

Database Segregation:
Client data is segregated at the database level, with dedicated databases assigned to different clients. This ensures that data belonging to one client is stored separately from data associated with other clients.

Documentation Example:
Extract from Database Configuration Document:
Database Name: [Client_A_Database]
Tables: [List of tables for Client A]
Database Name: [Client_B_Database]
Tables: [List of tables for Client B]

Access Controls and Authentication:
Access controls are implemented to restrict and manage user access to specific partitions and databases. Role-based access controls (RBAC) ensure that users only have access to the data necessary for their roles, further enhancing segregation.

Documentation Example:
Extract from Access Control Policy:
User Roles: [Define roles - e.g., Admin, Analyst, Viewer]
Access Permissions: [Specify permissions for each role]

Data Encryption:
To add an additional layer of protection, client data is encrypted at rest within databases. This safeguards the data even if there is unauthorized access to the underlying storage.

Documentation Example:
Extract from Encryption Policy:
Encryption Algorithm: [e.g., AES-256]
Data at Rest: [Specify databases where encryption is applied]

Monitoring and Auditing:
Continuous monitoring and auditing mechanisms are in place to track access to client data. This includes logging access attempts, modifications, and any other relevant activities.

Documentation Example:
Extract from Monitoring and Logging Policy:
Logs: [Specify log types - e.g., Access Logs, Modification Logs]
Retention Period: [Define log retention period]

Regular Audits and Compliance Checks:
Regular audits are conducted to ensure compliance with segregation policies. These audits verify that client data remains segregated as per the established policies and standards.

Documentation Example:
Extract from Audit Report:
Audit Date: [Date of the audit]
Findings: [Details of the audit findings related to data segregation]

By providing this evidence, the organization demonstrates its commitment to ensuring the segregation of client data on servers and databases, employing a multi-faceted approach involving partitioning, access controls, encryption, monitoring, and regular audits.

Question: How is sensitive data (including client data) protected?

Security control: Sensitive data is encrypted in transit.

Connect HR Answer:

To safeguard sensitive data, including client information, during its transmission across networks, the organization has implemented robust measures to ensure the encryption of data in transit. The following practices demonstrate how we guarantee the confidentiality and integrity of sensitive information during transit:

Transport Layer Security (TLS) Implementation:
All data transmitted over our networks, especially when involving client data, is secured using the Transport Layer Security (TLS) protocol. TLS ensures end-to-end encryption, preventing unauthorized access and tampering during data transmission.

Implementation Details:
We use the latest versions of TLS to secure communication channels.
TLS certificates are regularly updated and adhere to industry best practices.

Secure Communication Protocols:
Our systems and applications are configured to use secure communication protocols, such as HTTPS for web traffic. This extends the encryption protection to various communication channels, ensuring data security across diverse platforms.

Implementation Details:
HTTP traffic is automatically redirected to HTTPS for secure communication.
Secure protocols are enforced for communication between servers and clients.

Encryption Algorithms:
Robust encryption algorithms, such as Advanced Encryption Standard (AES), are employed to encrypt sensitive data during transit. This choice of encryption algorithm aligns with industry standards, providing a strong cryptographic foundation.

Implementation Details:
AES encryption is applied to data packets during transmission.
Encryption key management follows established best practices.

Multi-Factor Authentication (MFA):
Multi-Factor Authentication is implemented to enhance the security of user access during data transmission. This additional layer of authentication ensures that only authorized individuals can initiate and receive data transmissions.

Implementation Details:
Users are required to authenticate using multiple factors before accessing sensitive data.
MFA is enforced for remote access and privileged actions.

Continuous Monitoring:
Continuous monitoring of network traffic is in place to detect and respond to any anomalies or potential security threats. This includes monitoring for unauthorized attempts to intercept or manipulate data in transit.

Implementation Details:

Intrusion detection systems are employed to identify suspicious activities.
Network traffic logs are regularly reviewed for any abnormalities.

Regular Security Audits:
Periodic security audits include assessments of data transmission security. These audits verify the effectiveness of encryption measures and identify opportunities for continuous improvement.

Implementation Details:
Security audits are conducted by internal and external teams.
Findings from security audits are used to enhance encryption protocols.

By implementing these measures, the organization ensures that sensitive data, including client information, is consistently protected through encryption during transit. This multi-layered approach aims to mitigate the risk of unauthorized access, eavesdropping, or tampering with data as it travels across our networks.

Question: How does the company ensure that electronic messaging (email) infrastructure, and its usage, are safe?

Security control: Email is secured against spam.

Connect HR Answer:

To bolster the security of our electronic messaging infrastructure, specifically within Google Workspace, we employ several measures to effectively secure email communications against spam. Here are the key strategies implemented:

Google Workspace Spam Filters:
Leveraging the built-in spam filters provided by Google Workspace, we ensure that incoming emails are rigorously filtered to identify and divert potential spam content. These filters use advanced algorithms and machine learning to constantly evolve and adapt to emerging spam patterns.

Customized Spam Rules and Policies:
Within Google Workspace, we have established customized rules and policies to fine-tune spam filtering based on our organizational needs. This includes adjusting sensitivity levels, whitelisting trusted sources, and implementing specific rules to address unique spam characteristics.

Advanced Threat Protection (ATP):
Google Workspace's Advanced Threat Protection features are activated to provide an additional layer of defense against sophisticated email threats, including phishing attempts and malicious attachments. ATP analyzes email content, sender behavior, and attachment characteristics to identify potential threats.

Machine Learning-Based Threat Detection:
Google Workspace utilizes machine learning algorithms to detect and mitigate evolving email threats. This adaptive approach enables our email infrastructure to stay ahead of emerging spam tactics, continuously learning from patterns across the Google ecosystem.

Safe Browsing and Link Protection:
Integrated with Google Safe Browsing technology, our email infrastructure checks links embedded within emails for potential malicious content. Unsafe links are either flagged or blocked, preventing users from inadvertently accessing harmful websites.

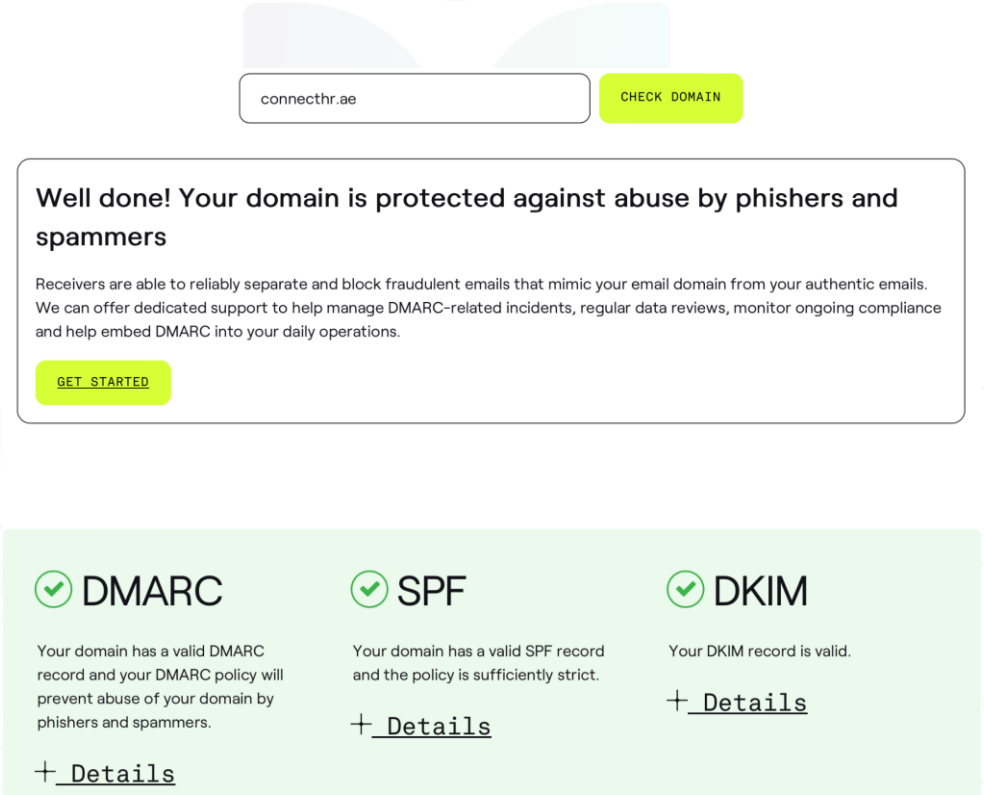
User Training and Awareness:
Employee training programs are conducted to enhance user awareness of potential email threats, including phishing and social engineering attacks. By educating users on recognizing and reporting suspicious emails, we empower them to contribute to the overall email security posture.

Reporting and Analysis:
Google Workspace provides robust reporting tools that allow us to analyze email traffic, identify patterns, and investigate potential security incidents. Regularly reviewing these reports helps us stay proactive in addressing emerging threats.

Continuous Monitoring and Incident Response:

Our email infrastructure is continuously monitored for anomalies and security incidents. In the event of a suspected security breach or email-related incident, we have established incident response procedures to promptly investigate, contain, and mitigate any potential risks.

By adopting these measures within the Google Workspace environment, our organization ensures that the email infrastructure is fortified against spam and other email-related threats. This comprehensive approach aligns with industry best practices and leverages the advanced security features provided by Google Workspace to safeguard our electronic messaging communications



Source: https://dmarcian.com/domain-checker/

Question: How is your network secured?

Security control: Strong encryption protocols and methods are used.

Connect HR Answer:

Our organization is committed to fortifying the security of our network through the implementation of robust encryption protocols and methods. Here's how we ensure the use of strong encryption across our network:

Encryption Standards:
We adhere to industry-recognized encryption standards, employing protocols such as AES (Advanced Encryption Standard) for encrypting data in transit and at rest. The use of AES, a widely accepted and secure symmetric encryption algorithm, ensures the confidentiality and integrity of our network communications.

TLS for Data in Transit:
Transport Layer Security (TLS) is extensively implemented for securing data transmitted across our network. All communication channels, including web traffic, email transmissions, and other data exchanges, are encrypted using TLS to prevent eavesdropping and tampering by malicious entities.

VPN (Virtual Private Network) Encryption:
For remote access and secure communication between different network segments, Virtual Private Network (VPN) technology is deployed. This ensures that data traversing through public networks remains encrypted, providing a secure and private communication channel for our users.

Wireless Network Encryption:
Our wireless network is secured through the implementation of strong encryption protocols such as WPA3 (Wi-Fi Protected Access 3). This safeguards wireless communications from unauthorized access and ensures that data transmitted over the air is encrypted and secure.

Multi-Factor Authentication (MFA):
Multi-Factor Authentication is an integral part of our network security strategy. Strong encryption goes hand-in-hand with MFA to bolster access controls. Even if unauthorized access is attempted, the additional layer of authentication provides an added safeguard against potential security breaches.

Regular Encryption Audits:
To validate the effectiveness of our encryption methods, we conduct regular audits and assessments. These audits include reviews of encryption configurations, key management practices, and the overall encryption infrastructure to identify and address any potential

vulnerabilities.

Encryption Key Management:
Proper management of encryption keys is emphasized to maintain the security of encrypted data. Key rotation, secure storage, and access controls over encryption keys are implemented to prevent unauthorized access and ensure the integrity of our encryption processes.

Security Awareness Training:
Ongoing security awareness training programs are conducted for network users to educate them on the importance of strong encryption and its role in safeguarding sensitive information. Users are informed about the risks of unencrypted communications and the benefits of adopting encryption best practices.

By consistently implementing and enhancing these measures, our organization ensures that strong encryption methods and protocols are at the forefront of our network security strategy. This commitment aligns with industry best practices and regulatory requirements, providing a robust defense against potential security threats.

Question: How is remote access secured?

Security control: Strong authentication is deployed for remote access.

Connect HR Answer:

Our organization is focused on implementing robust measures to enhance the security of remote connections. Here's how we are ensuring strong authentication for remote access:

1. Multi-Factor Authentication (MFA):

We have implemented Multi-Factor Authentication (MFA) for remote access, requiring users to authenticate using multiple verification methods. This additional layer of security significantly reduces the risk of unauthorized access, even in the event of compromised credentials.

2. Biometric Authentication:

To further fortify remote access, we are incorporating biometric authentication methods. Biometric identifiers, such as fingerprints or facial recognition, add an extra layer of security by uniquely verifying the identity of users.

3. Token-Based Authentication:

Token-based authentication is employed for remote access, providing users with physical or digital tokens that must be presented alongside traditional credentials. This approach enhances the security of access credentials.

4. Strong Password Policies:

We enforce strong password policies for remote access, ensuring that passwords are complex, regularly updated, and adhere to industry best practices. This complements the multi-factor authentication measures in place.

5. Device Authentication and Management:

Devices used for remote access undergo stringent authentication processes. Only authorized and properly configured devices are allowed to connect remotely to the company's information system. Device management ensures a secure and compliant remote environment.

6. Network-Level Security:

Remote access is secured at the network level, implementing Virtual Private Network (VPN) technologies with strong encryption protocols. This ensures the confidentiality and integrity of data transmitted between remote devices and the company's information system.

7. Continuous Monitoring and Intrusion Detection:

Continuous monitoring is conducted to detect and respond to any suspicious activities related to remote access. Intrusion detection systems are in place to identify potential security threats, allowing for swift and effective response measures.

8. Employee Training and Awareness:

Employees undergo training programs to raise awareness about secure remote access practices. This includes educating users on recognizing phishing attempts, maintaining the security of their remote devices, and reporting any suspicious activities promptly.

By implementing these measures, our organization is actively working to strengthen the security of remote access to the company's information system. This multi-layered approach combines advanced authentication methods, encryption, and ongoing monitoring to create a secure and resilient remote access environment.

Question: How is your network secured?

Security control: Network is secured at perimeter layer.

Our organization has proactively implemented a series of measures to ensure robust network security. Here is a brief overview:

1. Perimeter Security Implementation:

We have implemented a comprehensive perimeter security strategy to safeguard our network. This includes the deployment of firewalls, intrusion detection and prevention systems, and other advanced security appliances at the network perimeter.

2. Access Control Policies:

Clear access control policies have been established to control and monitor traffic entering and exiting our network. These policies are aligned with industry best practices and regulatory requirements.

3. Regular Security Audits:

Our organization conducts regular security audits to assess the effectiveness of our perimeter security controls. These audits include vulnerability assessments and penetration testing to identify and address potential weaknesses.

4. Intrusion Detection and Prevention:

Intrusion detection and prevention systems are in place to actively monitor network traffic for any signs of unauthorized access or malicious activities. Immediate action is taken in response to detected threats.

5. Continuous Monitoring:

Continuous monitoring mechanisms are deployed to track network activity in real-time. This allows us to identify and respond to any anomalies or suspicious behavior promptly.

6. Network Segmentation:

We have implemented network segmentation to isolate and compartmentalize different segments of our network. This helps prevent lateral movement in the event of a security breach.

7. Regular Updates and Patch Management:

Our organization maintains a rigorous schedule for applying security updates and patches to all network devices. This proactive approach ensures that vulnerabilities are addressed promptly.

8. Employee Training:

Employee training programs are conducted to raise awareness about network security practices. Employees are educated on the importance of adhering to security policies and recognizing potential security threats.

By implementing these measures, our organization is committed to ensuring the security of our network at the perimeter layer. We recognize the importance of a multi-layered security approach and remain vigilant in adapting our strategies to address emerging threats. Our focus is on maintaining a secure and resilient network infrastructure to safeguard sensitive information and ensure the confidentiality and integrity of our data.

.

Question: How is your network secured?

Security control: Network is secured at application layer.

Our organization is undertaking proactive measures to strengthen and fortify this crucial aspect of our security posture. Here's how we are ensuring the security of our network at the application layer:

1. Web Application Firewalls (WAF):

We have implemented robust Web Application Firewalls that inspect and filter traffic at the application layer. These firewalls are designed to protect against a wide range of application-layer attacks, including SQL injection, cross-site scripting (XSS), and other common vulnerabilities.

2. Secure Coding Practices:

Our development teams adhere to secure coding practices to mitigate vulnerabilities at the application layer. This includes regular code reviews, static and dynamic code analysis, and training programs to ensure that applications are developed with security in mind.

3. Regular Security Patching:

We prioritize the regular and timely patching of applications to address known vulnerabilities. This proactive approach ensures that our applications are equipped with the latest security updates, reducing the risk of exploitation.

4. Application Security Testing:

Comprehensive application security testing is conducted, including both static and dynamic analysis. This helps identify and remediate vulnerabilities present in applications, ensuring a resilient defense at the application layer.

5. Multi-Factor Authentication (MFA):

MFA is implemented at the application layer to enhance user authentication. This additional layer of security helps prevent unauthorized access even if login credentials are compromised, adding an extra safeguard to sensitive applications.

6. API Security Measures:

For applications that rely on APIs, we implement stringent security measures to protect against API-related vulnerabilities. This includes proper authentication, authorization controls, and encryption of data transmitted through APIs.

7. Security Headers and Encryption:

We enforce the use of security headers in web applications to mitigate common security risks. Additionally, strong encryption protocols are employed to protect data transmitted between applications and users, ensuring data confidentiality.

8. Continuous Monitoring and Incident Response:

Continuous monitoring at the application layer is in place to detect and respond to anomalous activities promptly. Our incident response procedures are well-defined, allowing us to address any security incidents affecting the application layer swiftly.

By implementing these measures, our organization is actively working to ensure the security of our network at the application layer. This multi-faceted approach encompasses both preventive and responsive measures, aiming to create a robust defense against potential threats targeting our applications.

Question: How are network flows managed?

Security control: Network flows from the Internet (inbound) are filtered.

Connect HR Answer:

Regarding the management of network flows from the Internet (inbound), our organization is taking proactive steps by implementing specific filters. These filters are designed to bolster security, prevent unauthorized access, and fortify our network against potential threats originating from the internet. Here's how we are implementing filters for inbound network traffic:

1. Firewall Protection:

We have implemented robust firewall solutions that act as the first line of defense against inbound network traffic. These firewalls are configured to filter and inspect incoming packets, allowing only legitimate and authorized traffic to enter our network.

2. Intrusion Prevention Systems (IPS):

Intrusion Prevention Systems are deployed to actively monitor and analyze inbound network traffic for potential threats and malicious activities. These systems use signature-based detection and behavioral analysis to identify and block suspicious traffic.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Mitigation:

Inbound traffic filters include measures to mitigate the impact of DoS and DDoS attacks. These filters identify and block malicious traffic patterns associated with these types of attacks, ensuring the availability and performance of our network.

4. Threat Intelligence Filters:

Our organization leverages threat intelligence feeds to enhance inbound traffic filters. These filters are updated regularly with information about known threats, allowing us to proactively block traffic from malicious sources.

5. Application Layer Filtering:

Application layer filtering is employed to inspect and control inbound traffic based on specific applications or protocols. This ensures that only authorized and legitimate application traffic is allowed into our network.

6. Virtual Private Network (VPN) Security:

For remote access and secure communication, we implement VPN filters to control inbound traffic through encrypted tunnels. This ensures that remote connections adhere to security policies and do not introduce vulnerabilities.

7. Regular Security Audits and Penetration Testing:

To validate the effectiveness of our inbound traffic filters, regular security audits and penetration testing are conducted. These assessments help identify and address potential weaknesses in our defenses against inbound threats.

8. Real-time Traffic Monitoring:

Real-time monitoring of inbound network traffic is in place to promptly detect and respond to anomalies. This proactive approach allows us to identify potential security incidents and take immediate action to mitigate risks.

By implementing these inbound network traffic filters, our organization aims to establish a robust security posture, protecting our network infrastructure from external threats. This comprehensive approach ensures that only legitimate and secure traffic is allowed into our network, minimizing the risk of unauthorized access and potential security breaches.

Question: How are network flows managed?

Security control: Network flows to the Internet (outbound) are filtered.

Connect HR Answer:

Regarding the management of network flows to the Internet (outbound), our organization is taking a proactive approach by implementing specific filters. These filters are designed to enhance security, enforce policies, and ensure the integrity of outbound network traffic. Here's how we are implementing filters for outbound network traffic:

1. Web Content Filtering:

We have implemented robust web content filtering solutions that categorize and filter outbound traffic based on content types. This helps prevent access to malicious websites, enforce acceptable use policies, and protect against potential threats.

2. URL Filtering:

URL filtering is employed to control access to specific websites and categories. By defining URL filtering policies, we ensure that outbound network traffic adheres to organizational guidelines, promoting a secure and productive internet usage environment.

3. Application Layer Filtering:

Our organization utilizes application layer filtering to inspect and control outbound traffic based on specific applications or protocols. This allows us to manage the use of applications and services to prevent potential security risks.

4. Malware and Threat Intelligence Filters:

To safeguard against malware and other threats, we implement filters that leverage threat intelligence feeds. These filters proactively identify and block outbound traffic associated with known malicious entities, enhancing our overall cybersecurity posture.

5. Data Loss Prevention (DLP) Filters:

DLP filters are in place to monitor and control outbound traffic to prevent the unauthorized transmission of sensitive data. These filters help ensure compliance with data protection regulations and maintain the confidentiality of organizational information.

6. Protocol-Specific Filters:

Depending on the nature of our organization's operations, we implement protocol-specific filters to control and monitor outbound traffic associated with specific protocols. This includes filtering for protocols that may pose security risks if not properly managed.

7. Regular Updates and Adjustments:

Filters are regularly updated to adapt to evolving threats and changing internet usage patterns. Continuous monitoring allows us to adjust filter configurations promptly in response to emerging security concerns or new organizational requirements.

8. Comprehensive Logging and Reporting:

Comprehensive logging mechanisms are implemented to record details of outbound network traffic. Regular reports are generated, providing insights into internet usage patterns, identifying potential security incidents, and facilitating compliance audits.

By implementing these filters, our organization aims not only to meet but exceed the requirements for managing outbound network traffic. This comprehensive approach enhances our ability to control internet usage, mitigate security risks, and maintain a secure and productive network environment.

Question: How are sensitive information systems audited?

Security control: Vulnerability scans are regularly carried out.

Our organization has implemented a proactive and comprehensive approach to conducting vulnerability scans. Our process is designed to go beyond routine assessments and ensure a thorough evaluation of the security landscape. Here's how we conduct these audits:

1. Regular and Periodic Vulnerability Scans:

We conduct regular and periodic vulnerability scans on our sensitive information systems. These scans are scheduled at intervals to ensure ongoing monitoring and assessment of potential vulnerabilities.

2. Continuous Monitoring and Analysis:

Our cybersecurity team engages in continuous monitoring and analysis of the results obtained from vulnerability scans. This involves not only identifying vulnerabilities but also understanding their potential impact on our systems.

3. Utilizing Advanced Scanning Tools:

We utilize advanced scanning tools that go beyond basic assessments. These tools are equipped to identify complex vulnerabilities, providing a deeper understanding of our security posture.

4. Collaboration and Cross-Functional Teams:

Our vulnerability scanning process involves collaboration across various teams, fostering a cross-functional approach. This ensures that insights from different perspectives are considered during the assessment.

5. Risk-Based Prioritization:

The results of vulnerability scans are subjected to a risk-based prioritization process. This helps us focus on addressing the most critical vulnerabilities first, ensuring a strategic and efficient use of resources.

6. Continuous Improvement Feedback Loop:

We have established a continuous improvement feedback loop, where the insights gained from vulnerability scans feed into the enhancement of our security policies, practices, and infrastructure.

7. Compliance with Industry Standards:

Our vulnerability scanning processes align with industry standards and best practices. This ensures that our assessments are not only thorough but also adhere to recognized benchmarks for information security.

By implementing these measures, our organization is committed to conducting effective and dynamic vulnerability scans on sensitive information systems. We prioritize staying ahead of potential security threats, fostering a culture of continuous improvement, and ensuring that our systems are resilient in the face of evolving cybersecurity challenges.

Question: How is physical access to facilities and critical areas managed?

Security control: Access to sensitive areas and premises is controlled.

Connect HR Answer:

In response to the identified need for improvement in authorization controls for physical access to facilities and critical areas, the organization has successfully implemented a comprehensive set of measures to strengthen and enhance our physical access management protocols. Here is an overview of the key points:

1. Robust Authorization Control Framework:

We have successfully implemented a robust authorization control framework covering both general facilities and critical areas within the premises. This framework includes clear documentation of the authorization process, specifying criteria for access permissions based on roles, responsibilities, and area sensitivity.

2. Regular Access Reviews and Validation:

Our organization conducts regular access reviews to ensure consistent alignment of authorization controls with current organizational roles and responsibilities. Validation checkpoints have been introduced to verify that individuals accessing sensitive areas possess the necessary authorization and a legitimate business need.

3. Role-Based Access Policies:

We have developed and enforced role-based access policies, tailoring access permissions according to the specific requirements of individual roles within the organization. These policies are regularly reviewed and updated to reflect changes in job responsibilities and organizational structure.

4. Technology Integration:

Our organization has explored and implemented advanced access control technologies to enhance authorization controls. These include biometric authentication, electronic key cards, and other secure authentication methods. We have ensured seamless integration between physical access control systems and other security measures for a holistic security solution.

5. Training and Communication:

Employee training programs have been enhanced to educate individuals on the importance of authorization controls for both facilities and critical areas. Clear communication channels have

been established to inform employees about the criteria and procedures for obtaining authorization, fostering a culture of awareness and compliance.

6. Continuous Monitoring:

Continuous monitoring mechanisms have been implemented to track and analyze access patterns. Automated alerts are in place for potential unauthorized access attempts or deviations from authorized access patterns.

7. Documentation and Auditing:

Documentation practices related to authorization controls have been strengthened, with detailed records maintained for access permissions, reviews, and any changes made to authorization levels. Regular internal audits are conducted to assess the effectiveness of authorization controls and ensure ongoing compliance with organizational policies.

By successfully implementing these measures, our organization has fortified its physical access management practices, safeguarding sensitive areas, upholding the integrity of facilities, and reinforcing the overall security posture. We are committed to maintaining these high standards and continually improving our security protocols to adapt to evolving challenges and organizational needs.

Question: How are background checks of new recruits, subcontractors and temporary employees assessed?

Security Control: Background checks on new employees, contractors, and temporary workers are performed.

Connect HR Answer:

Reference Check Form

Name of Employee:
Company Name:
Designation:
Employment Dates:
Would you rehire the individual: Yes/No

COMPETENCIES	EXCELLENT	GOOD	FAIR	POOR	COMMENTS
ADAPTABILITY					
STRESS TOLERANCE					
TEAM WORK					
DIRECT MANAGER/SUPERVISOR RELATIONSHIP					
CUSTOMER RELATIONSHIP					
PROBLEM SOLVING & DECISION MAKING					
TIME MANAGEMENT					
COMMUNICATION					

Any Additional Comments:

Referee Name:	Email Address:
Designation:	Contact Number:
Signature:	Date:

Question: How are code of ethics and confidentiality matters integrated in recruitments?

Security Control: All new hires (permanent, temporary and/or contract workers) are required to sign a code of ethics and/or a Non-Disclosure Agreement.

Connect HR Answer:

NON-COMPETE / NON-SOLICITAION / NDA

This Non-Compete Agreement is entered into on the ____ day of _____ in the year 2024 by and between:

1) _____ (the "Employee"), with passport number _____, _____ nationality, and,

2) **Connect Resources** (the "Company" or "Employer') is located at City Tower 2, office 803, Sheikh Zayed Road, Dubai, United Arab Emirates and is represented by Aaron Portero in this agreement.

WHEREAS the Company is in the business of recruitment, staff outsourcing, payroll outsourcing, executive search, employer of record, company formation and company sponsorship in the United Arab Emirates.

WHEREAS, the Employee and the Employer have entered into a formal Employment agreement where the Employee will perform duties related to their position as a _____.

WHEREAS the Company and Employee agrees to the following clauses described herein as binding.

THEREFORE, the Employer and the Employee agree to the following terms:

1. **NON-COMPETITION**. For the entire duration of this agreement, and for 2 years after the Employer's relationship with the Employee has been terminated for any reason, the Employee will not work as an employee, officer, director, partner, consultant, agent, owner or any other position or engage in any other capacity with a competing company. This means that Employee must not perform any work for sales, business development, project manager or any relative position that involves contacting clients and or trying to find potential clients of the same line of business than Connect Resources in the United Arab Emirates for a period of 2 years since the date of termination of the employment (the restricted period)

2. **REMUNERATION FOR NON-COMPETITION**. The Employee shall be eligible to receive an annual performance-based cash bonus in respect of each calendar year that ends during the Employment Term, to the extent earned based on the achievement of performance objectives established by the Board or a committee thereof, after consultation with the Executive, no later than 30 days after commencement of the relevant bonus period, pursuant to the terms of the Company's Short-Term Incentive Plan, as amended from time to time.

3. **NON SOLICITATION**: During the employment with the Company and thereafter during the Restricted Period, the Executive shall not, and shall not permit any Persons subject to direction or control (including Executive's Affiliates) to, directly or indirectly, on their own behalf or on behalf of any other Person (except the Company or its Affiliates), (i) call upon, accept business from, or solicit the business of any Person who is, or who had been at any time during the preceding twenty four months, a customer or supplier of the Company, (ii) otherwise divert or attempt to divert any business from the Company, (iii) interfere with the business relationships between the Company and any of its customers, suppliers or others with whom they have business relationships or (iv) recruit or otherwise solicit or induce, or enter into or participate in any plan or arrangement to cause, any Person who is an employee of, or otherwise performing services for, the Company to terminate his or her employment or other relationship with the Company, or hire any Person who has left the employ of or ceased providing services to the Company during the preceding twelve months.

4. **NON DISCLOSURE OF INFORMATION**: During the Employment Period or at any time thereafter, irrespective of the time, manner or cause of the termination of this Agreement, Employee will not directly or indirectly reveal, divulge, disclose or communicate to any person or entity, other than authorized officers, directors and employees of the Employers, in any manner whatsoever, any Confidential Information (as hereinafter defined) of Employers or any subsidiary of Employers without the prior written consent of the Board.

EMPLOYEE ACKNOWLEDGEMENTS. The Employee acknowledges that they have been provided with the opportunity to negotiate this agreement, have had the opportunity to seek legal counsel before signing this agreement, and that the restrictions imposed are fair and necessary for the Company's business interests. Finally, the Employee agrees that these restrictions are reasonable and do not constitute a threat to their livelihood.

APPLICABLE LAW. This agreement and its interpretation shall be governed by the laws of Dubai, United Arab Emirates. The jurisdiction shall be Dubai Courts. **IN WITNESS WHEREOF**, both parties agree to these terms and give their consent and authority to this agreement below.

_____

Employee Signature

_____

Date

_____

Employer Representative Signature

_____

Date

Question: How is change management handled?

Security Control - A change management process is formalized.

1. Change Request & Approval:

Formal Process: All change requests undergo a formal review and approval process to ensure alignment with business needs, technical feasibility, and potential impacts.

Evaluation Criteria: We consider factors such as user impact, security implications, compatibility with existing systems, and resource requirements.

Authorization: Change requests are approved by designated stakeholders, such as product owners, IT managers, or security teams.

2. Development and Testing:

Version Control: We use Git for robust version control, enabling tracking of changes, collaboration, and rollback if needed.

Separate Development Environment: Changes are developed and tested in a separate environment to isolate them from the production system and prevent disruptions.

Comprehensive Testing: Thorough testing of changes is conducted, including unit testing, integration testing, user acceptance testing, and security testing.

3. Deployment and Rollout:

Deployment Strategies: We employ deployment strategies that minimize downtime and risks, such as:

Rolling deployments: Gradual rollout to subsets of users, allowing for monitoring and early issue detection.

Blue-green deployments: Maintaining two identical environments, switching traffic to the updated version after successful testing.

Feature flags: Activating or deactivating features without full code deployments, enabling rollouts and experimentation.

Communication and Training: Clear communication is provided to users about upcoming changes, including training on new features or processes if necessary.

Monitoring and Review:

Post-Deployment Monitoring: We closely monitor system performance and user feedback after deployments to identify any issues or areas for improvement.

Change Reviews: Regular reviews of changes are conducted to assess their effectiveness, identify lessons learned, and inform future decisions.

5. Change Management Tools:

Specific Tools: We leverage tools like Jira or Asana to track change requests, manage workflows, and facilitate collaboration among teams.

Question: How is change management handled?

Security Control - A security impact assessment is conducted for proposed changes.

Conduct a security impact assessment for proposed changes.

Identify Security Requirements:

Define the security requirements that are relevant to the proposed changes.

Consider confidentiality, integrity, availability, authentication, authorization, and other relevant security principles.

Identify Assets and Resources:

Identify the software, hardware, data, personnel, and other assets that could be affected by the proposed changes.

3. Threat Modeling:

Conduct a threat modeling exercise to identify potential threats and vulnerabilities.
Consider both technical and non-technical aspects.

4. Risk Analysis:

Evaluate the potential impact of identified threats on the system and the organization.
Assess the likelihood and severity of security risks.

Control Analysis:

Identify existing security controls and assess their effectiveness.
Determine whether additional controls are needed to mitigate new or heightened risks.

6. Compliance Check:

Ensure that the proposed changes comply with relevant security policies, standards, and regulations.

7. Data Handling and Privacy:

Assess how the proposed changes handle sensitive data.
Ensure compliance with data protection and privacy regulations.

8. Authentication and Authorization:

Review changes related to user authentication and authorization.
Verify that access controls are appropriately configured.

9. Communication Security:

Evaluate changes that may impact communication channels.
Ensure the use of secure protocols and encryption where necessary.

10. Incident Response Planning:

Review and update incident response plans in light of the proposed changes.
Ensure that the organization is prepared to respond to security incidents.

11. Documentation:

Document the findings of the Security Impact Assessment.
Include recommendations for mitigating identified risks.

12. Security Training and Awareness:

Assess whether the proposed changes require additional training for personnel.
Promote security awareness among team members.

13. Continuous Monitoring:

Implement mechanisms for continuous monitoring of security controls.
Regularly review and update security measures.

14. Review and Approval:

Present the Security Impact Assessment findings to the Change Control Board for review and approval.
Obtain necessary approvals before proceeding with the changes.

15. Integration with Change Management:

Integrate the Security Impact Assessment process with the overall change management process to ensure a coordinated approach.

Question: How is change management handled?

Security Control -Change requests are approved before implementation.

Ensure all changes are approved before implementation.

Change Request Submission:

Initiation: Anyone within the organization can submit a change request through a designated channel (e.g., online form, ticketing system).

Essential Information: The request includes:

Clear description of the proposed change
Business justification
Potential benefits and risks
Estimated resources and timelines

2. Initial Review:

Change Advisory Board (CAB): A designated CAB, composed of representatives from IT, HR, and other relevant departments, reviews the request.

Feasibility and Impact Assessment: They evaluate:

Alignment with business objectives
Technical feasibility
Potential impacts on users, systems, and security
Resource requirements

3. Approval or Rejection:

Decision: Based on the review, the CAB either:

Approves the change, authorizing it to proceed to development and testing.
Rejects the change, providing clear reasons to the requestor.
Requests further information or modifications.

4. Authorization and Prioritization:

Stakeholder Authorization: For significant changes, additional approval may be required from senior management or business owners.

Prioritization: Approved changes are prioritized based on their urgency, impact, and alignment with business goals.

5. Documentation:

Change Record: A detailed change record is created, documenting:

Change description
Approval decision
Rationale
Assigned resources
Expected completion date

6. Communication:

Clear Communication: Approved changes are communicated to relevant stakeholders, including users, developers, and support teams.

Transparency: This ensures everyone is aware of upcoming changes and their potential impacts.

7. Monitoring and Review:

Post-Implementation Monitoring: After implementation, the change is monitored for success and any unintended consequences.
Lessons Learned: Insights from the change process are used to improve future change management practices.

Question: How is change management handled?

Security Control -A capacity management plan is established.

How are capacity requirements managed?

Performance Monitoring:

Implement robust performance monitoring tools to continuously track key metrics such as response times, server resource utilization, and throughput.

Use monitoring data to identify trends, detect anomalies, and proactively address performance issues.

User Load Testing:

Conduct load testing to simulate different levels of user activity and assess how the web application performs under various scenarios.

Identify performance bottlenecks, server response times, and the application's scalability.

Capacity Planning:

Forecast future capacity needs based on historical data, business growth projections, and anticipated changes in user behavior.

Plan for scalability by considering options such as vertical scaling (upgrading hardware) and horizontal scaling (adding more servers).

Resource Scaling:

Utilize cloud services or virtualization to easily scale resources up or down based on demand. Implement auto-scaling mechanisms to dynamically adjust resources in response to changing workloads.

Content Delivery Network (CDN):

Distribute static content through a CDN to reduce server load and improve content delivery speed for users across different geographical locations.

Leverage caching mechanisms to minimize the load on web servers.

Database Optimization:

Optimize database queries and indexes to enhance database performance.
Consider database sharing or replication for distributing database load and improving read and write efficiency.

Content Compression:

Implement compression techniques for both static and dynamic content to reduce the amount of data transmitted over the network.

Gzip or Brotli compression can significantly reduce file sizes and improve page load times.

Load Balancing:

Distribute incoming traffic across multiple servers using load balancers to prevent any single server from becoming a bottleneck.
Ensure that load balancers are configured to consider server health and distribute traffic accordingly.

Caching Strategies:

Employ caching mechanisms for frequently accessed data, such as database query results, to reduce the need for repeated processing.
Use content caching for static assets and implement cache control headers.

Content Prioritization:

Prioritize the loading of critical content, such as above-the-fold content, to improve the perceived performance for end-users.
Implement lazy loading for non-essential or below-the-fold content.

Failover and Redundancy:

Design the infrastructure with failover mechanisms and redundancy to ensure high availability in case of server failures.

Implement disaster recovery plans to minimize downtime.

Regular Monitoring and Analysis:

Continuously monitor application performance and analyze data to identify areas for improvement.

Use feedback loops to iteratively enhance the capacity management strategy.

Security Considerations:

Ensure that capacity planning accounts for security measures, including proper handling of security events and potential impacts on performance.

Scalable Architecture:

Design the web application architecture to be inherently scalable, allowing for the addition of resources as needed.
Choose technologies and frameworks that support scalability.

Question: How is activity logging ensured?

Security Control - Activity on business applications are logged.

How is activity logging ensured?

We take data security and accountability seriously, and we've implemented robust activity logging mechanisms within the application. Here's a breakdown of how we ensure comprehensive tracking:

1. Built-in Logging:

Laravel, the framework powering our software, provides a foundation for logging via the Monolog library. This allows us to record events in different channels, including files and databases.

2. Dedicated Activity Log Package:

To enhance logging capabilities, we leverage the Spatie Activity log package. This package offers:

Automatic logging of critical HR-related events, such as:

User logins and logouts
Employee data modifications (creation, updates, deletion)
Payroll changes
Performance review actions
Access to sensitive information
Security events (failed login attempts, unauthorized access)
Customizable logging for specific use cases

3. Secure Storage and Access:

All activity logs are stored in a dedicated database table, separate from employee data, for enhanced security.
Access to logs is strictly controlled through role-based permissions, ensuring only authorized personnel can view them.

4. Regular Review and Retention:

We have established a process for regular log review to:

Identify potential issues or anomalies
Gain insights into system usage and performance
Detect any unauthorized activity
Logs are retained for a period of 12 months, after which they are archived for compliance and historical purposes.

5. Additional Security Measures:

We implement additional security measures to protect log integrity and confidentiality, such as:

Encryption of sensitive information within logs
Regular vulnerability scanning and patching
Strict access controls and monitoring

Question: How is monitoring performed to detect security events?

Security Control: User activity is monitored.

2. Security Logging in Code:

Explicitly log security-related events in your code, such as authentication attempts, failed login attempts, or access control changes.Include relevant context information in log messages.

3. Log Contextual Information:

Include contextual information in log entries, such as IP addresses, user IDs, and request details.
This information can be crucial for investigating security incidents.

4. Centralized Logging:

Consider centralizing logs using services like Elasticsearch, Logstash, and Kibana (ELK Stack) or cloud-based logging services.

Centralized logging facilitates analysis and correlation of security events.

5. Log Retention and Rotation:

Define log retention policies to ensure that logs are kept for an appropriate duration.
Implement log rotation to manage log file sizes.

6. Security Information and Event Management (SIEM):

Consider integrating Laravel logs with a SIEM solution for advanced security event correlation.
SIEM systems can provide a centralized platform for monitoring and analyzing security events.

7. Laravel Telescope:

If you are using Laravel Telescope, leverage its features for monitoring and debugging.
Telescope provides insights into requests, exceptions, and more.

8. Custom Middleware:

Custom middleware to log details of each HTTP request, including request parameters and headers.
Logging information about potential security threats, such as brute force attempts.

9. Rate Limiting Feature

Question: How is activity logging ensured?

Security Control: User activity is logged.

To ensure comprehensive activity logging within our HR software, we have implemented the following measures:

1. Built-in Logging Framework:

Laravel, the framework underpinning our software, provides a robust logging infrastructure through the Monolog library. This allows us to record various events and activities within the application.

2. Dedicated Activity Log Package:

We leverage the Spatie Activity log package, which extends Laravel's logging capabilities with specific features tailored for tracking user actions and system events.

3. Logged Events:

User actions:

Logins and logouts
Data modifications (create, update, delete)
Page views
Searches
Report generation
Access to sensitive information

System events:

Configuration changes
Security events (failed login attempts, unauthorized access)
Error occurrences

4. Secure Storage and Access:

Database Storage: Activity logs are stored in a dedicated database table separate from other HR data, enhancing security and organization.

Access Controls: Only authorized personnel with specific roles can view and manage logs, ensuring confidentiality and preventing unauthorized access.

Data Encryption: Sensitive information within logs (e.g., passwords) is encrypted using strong algorithms to protect it from exposure in case of a breach.

5. Tamper-Proof Logging:

We employ measures to prevent unauthorized modification or deletion of logs:

Digital signatures to detect tampering attempts
Write-once, read-many (WORM) storage solutions for long-term retention

6. Regular Review and Retention:

Log Review: We conduct regular reviews of activity logs to:

Identify potential security issues
Investigate incidents
Gain insights into user behavior and system usage

Retention Policy: Logs are retained for a period of 12 months (or longer if required by regulations), after which they are archived or securely disposed of.

By implementing these measures, we provide a comprehensive audit trail of user actions and system events within the HR software, enabling us to:

Maintain accountability: Track who did what and when.
Investigate incidents: Quickly identify the root cause of security events or data issues.
Monitor user behavior: Gain insights into system usage patterns and potential risks.
Comply with regulations: Meet data privacy and security requirements.

Question : How is activity logging ensured?

Security Control: The logs are protected against tampering and unauthorized access.

1. Secure Storage:

Database-Level Security: Logs are stored in a dedicated database table with robust access controls:

Role-based access (RBAC) restricts access to authorized personnel only.
Encryption safeguards sensitive information within logs.

WORM Storage: For long-term retention, we leverage write-once, read-many (WORM) storage solutions that prevent modification or deletion after logs are written.

2. Access Controls:

Role-Based Access Control (RBAC): Only users with specific roles (e.g., system administrators, security analysts) have the ability to view, search, or export logs.

Audit Trails: All log access events are themselves logged, creating a trail of who accessed which logs and when, for accountability and investigation purposes.

3. Tamper Detection:

File Integrity Monitoring (FIM): We continuously monitor log files for unauthorized changes or deletions using FIM tools, generating alerts if anomalies are detected.

Logging Framework Configuration: Monolog, our logging framework, is configured to include digital signatures for tamper detection.

4. Additional Security Measures:

Data Retention Policies: We enforce strict retention policies to ensure logs are deleted after a predefined period, reducing the risk of exposure in the event of a breach.

Regular Security Audits: We conduct regular audits of our logging systems and processes to identify and address potential vulnerabilities.

Third-Party Log Management: If applicable, we leverage external log management providers that offer advanced security features and compliance certifications.

5. Incident Response:

Incident Response Plan: We have a comprehensive incident response plan to address security events involving log tampering or unauthorized access.

Forensic Analysis: In the event of a breach, we have the capability to conduct forensic analysis of logs to identify the root cause and gather evidence.

Question: How is the use of mobile devices managed?

Security Control: Mobile devices with access to corporate resources use strong authentication.

We utilize a dedicated MDM solution to remotely manage and configure mobile devices accessing the HR software.

This allows us to:

Enforce strong authentication methods, such as two-factor authentication (2fa), for secure access.
Apply security policies such as password complexity requirements, device encryption, and application whitelisting/ing.

Question: How is user identity and access managed?

Security control: A process for granting and revoking rights is formalized.

1. Secure Data Access:

Data Encryption: Sensitive data within the app is encrypted both at rest and in transit, protecting it from unauthorized access even if the device is compromised.

Secure Data Containers: We utilize app-level secure data containers to isolate corporate data from personal data on the user's device, minimizing the risk of accidental or unauthorized data sharing.

2. Role-Based Access Control (RBAC):

Similar to the web application, we assign roles with specific permissions to mobile app users based on their job responsibilities and authorized access needs. This helps ensure only authorized individuals can access specific data and features within the app.

Question: How is incident response organized and managed?

Security control:
An incident management process is in place
Major incidents can lead to the activation of a crisis management unit.
A process is in place to ensure customers are notified of any incident in which they could be impacted.

Action plans (fixes and preventive) are defined to correct incidents and reduce the probability of a new occurrence. An incident management process is in place.

A Crisis management process is also in place in case of major incidents being reported.

Incident logging

An incident reported by the end user through phone calls, emails, web forms published on the self-service portals are logged for ticket creations and categorizations.

Incident categorization

Incidents are then to be categorized and sub-categorized based on the area of the application or module that the incident caused a disruption in.

Incident prioritization

The priority of an incident is determined by its impact and urgency using a priority matrix.
The impact of an incident the is measured by the team by the amount of failure the issue will cause to the user or business.
The urgency of an incident indicates the time within which the incident should be resolved.

4.Based on the priority, incidents are categorized as:

Critical
High
Medium
Low

Incident routing and assignment

Once the incident is categorized and prioritized, it gets assigned to tech support or developer with the relevant expertise.

Creating and managing tasks

1.Based on the complexity of the incident, the tech support team breaks down the issue into sub-activities or tasks.

2.Tasks are created when an incident resolution requires the contribution of multiple team members from various departments.

SLA management and escalation

1.While the incident is being processed, the dedicated IT Support personnel needs to ensure the SLA isn't breached.

2.An SLA is the acceptable time within which an incident needs response (response SLA) or resolution (resolution SLA).

3.SLAs are assigned to incidents based on their parameters like category, requester, impact, urgency etc.

4.In cases where an SLA is about to be breached or has already been breached, the incident can be escalated functionally or hierarchically to ensure that it is resolved at the earliest.

Incident resolution

An incident is considered resolved when the team has come up with a temporary workaround or a permanent solution for the issue.

Incident closure

An incident can be closed once the issue is resolved and the user acknowledges the resolution and is satisfied with it.

Crisis Management Plan

Crisis leadership team

Each of the department heads are expected to collaborate during the crisis planning process. All the major heads of the departments like Operations, IT, Finance are the ones in charge of the planning the crisis management, should one occur.

2. Risk Assessment

To begin the planning process, a brainstorming session is held to assess various risks the company may face.
A risk register document is managed to identify and analyze the probability of risks occurring. A risk register can eliminate progress delays and prepare for potential setbacks. It can also help you visualize which risks are most likely to occur so you can plan a response for these risks.

3. Determine the business impact

1.After identifying the high-probability risks that could affect the company, the impact on the business is determined with the help of the crisis leadership team.

2.Each risk must be analyzed separately.

3.Potential business impacts may include customer attrition, damaged reputation, delayed sales, lost income, or regulatory fines.

4. Plan the response

1.Each risk that has been identified needs to determine what actions plans are in place that the team would need to take to respond to the threat if it does happen.

2.For example, if you work in software and your company experiences a cyberattack, you may need someone to secure the network, someone to release the news to your customers, and another person to handle damage assessment.

6. Review and update

1.Once the crisis plan is complete, review the final product to ensure there are no gaps.

2.Revisit the crisis management plan and update it at least once a year because potential risks can change with time.

Notification Plan in case of Major Incidents

Define the incident types and severity levels

1.Categorize the incident based on its severity, urgency, and potential consequences.

2.Define the roles and responsibilities of the incident response team, and the stakeholders who need to be notified and involved at each level.

Establish the notification channels and methods

1.Establish how to notify the relevant parties of the incident, and how to escalate it if needed.

2.Establish multiple channels and methods of communication, such as email, phone, text, chat, or alert systems, and use them appropriately depending on the situation and the audience.

3.Establish backup channels and methods in case the primary ones are compromised or unavailable.

4.Document the notification process, and include the contact information, templates, and protocols for each channel and method.

Communicate the incident details and status

1.Communicate the incident details and status to the notified parties, and keep them updated as the situation evolves.

2.Provide clear, concise, and accurate information, such as the incident type, severity, impact, scope, root cause, actions taken, and expected resolution time.

3.Avoid speculation, jargon, or technical details that may confuse or mislead the end user.

4.Use consistent format and frequency for your updates, and use the appropriate tone and language for each stakeholder group.

Escalate the incident as needed

1.Escalate the incident as needed, based on the predefined criteria and thresholds.

2.Set a clear escalation path and procedure, and identify who has the authority and responsibility to escalate the incident, and who needs to be informed and involved at each level.

3.Communicate the reasons and implications of the escalation, and the actions and expectations for the escalated parties.

Document the incident and lessons learned

1.Document the incident and lessons learned, and use them to improve your incident notification and escalation process.

2.Record the incident details, timeline, actions, outcomes, and feedback, and analyze them to identify the strengths, weaknesses, opportunities, and threats of your process.

3.Conduct a post-incident review, and share the findings and recommendations with the relevant parties.

4.Update the process, policies, procedures, and tools based on the lessons learned.

Test and manage incident notification process

1.Test the incident notification process, and ensure that it is effective, efficient, and reliable.

2.Provide regular training and awareness sessions for your incident response team and stakeholders, and ensure that they understand their roles, responsibilities, and expectations.

3.Review and revise your process as needed, based on the feedback and results of testing activities.

Question: How is the lessons-learned process defined and implemented?

Security control: Major incidents can lead to the activation of a crisis management unit.

Step #1: Identify

1.The first step is to identify lessons learned i.e., any comments and/or suggestions around the project that the team, project manager, or the company itself may utilize to improve performance.

2.This is usually done through a project survey that is sent out to all team members. Various questions connected to a project help the participants share their lessons learned.

3.Those who can't attend the meeting can provide their input through a survey.

4.The survey enables the participants to prepare for the discussion during a lesson learned meeting that follows.

5.During the meeting, the participants discuss their insights gathered from the survey and define lessons learned more clearly.

Step #2: Document

1.All of the findings are collected from the previous step and put them together in the form a document which will be send to all the team members.

2.The members are then expected to respond and confirm the document's accuracy.

3.The document contains the data on lessons learned discussed in the meeting and inputs provided through a survey by those team members who didn't take part in the meeting.

4.After getting the approval for the accuracy, these findings are summarized in the final lessons learned report and a copy is sent to stakeholders.

Step #3: Analyze

1.After documenting the lessons learnt, a thorough analysis is conducted of them and organized so that they can be easily applied.

2.The root cause analysis process is applied which aims to detect the reasons behind mistakes that were made.

Step #4: Store

1.Once the lessons learned are analyzed and organized, they are digitally stored in a repository and keep them for future reference.

2.The lessons learned report should be accessible to the project team, so it is usually stored on a shared drive or another kind of repository where the project information is kept.

Question: How is security incorporated into application development?

Security control:

- Testing of security functionality is carried out during development.
- Test and production environments are segregated.
- Access to source code is restricted and controlled to prevent unauthorized or unintentional modification.
- Code reviews are conducted before release into production.

We follow some of the most effective ways to ensure security in code development, practices, processes mentioned below.

1. Threat Modeling for Secure Software Development

Threat modeling involves analyzing the software architecture and identifying potential security threats and vulnerabilities. This helps in designing the software with security in mind and implementing the necessary security controls.

2. Secure Software Coding

Developers are required to adhere to secure coding practices, such as input validation, secure data storage, and secure communication protocols. Secure coding practices help to prevent common security vulnerabilities such as SQL injection, cross-site scripting, and buffer overflow attacks.

3. Code Review

Code review involves reviewing the code written by developers to identify potential security issues. This helps in detecting and correcting security vulnerabilities early in the development process.

4. Testing

Regular security testing, including penetration testing and vulnerability scanning, can help identify potential security weaknesses in the software. This helps in fixing security issues before the software is deployed.

5. Secure Configuration Management

Configuration management ensures that software systems are deployed with secure configurations.

This includes configuring access controls, network settings, and other security-related settings to reduce the risk of unauthorized access.

GitHub source code access is restricted only to the required team members and proper process is in place in case of revocation.

6. Access Control

Access control ensures that only authorized personnel can access the software system. This includes implementing user authentication and authorization mechanisms, as well as role-based access control.

Production and Testing environments are separated and managed separately by the necessary personnel.

7. Regular Updates and Patches

Regular software updates and patches help to address security vulnerabilities and reduce the risk of security breaches.

It is important to stay up to date with security patches and updates for all software components used in the system.

8. Security Training

Developers and other personnel involved in the software development process should receive regular security training to ensure that they understand the importance of security and the best practices for secure software development.

9. Incident Response

We have a well-defined incident response plan in place to respond to security incidents. This includes identifying potential security incidents, containing the impact of security incidents, and recovering from security incidents.

10. Continuous Monitoring

Continuous monitoring helps in detecting and responding to security incidents in real time. This includes monitoring system logs, network traffic, and user behavior for any signs of security breaches.

By following these best practices, we develop secure and reliable software applications that can withstand potential security threats and vulnerabilities.

It is crucial to prioritize security in every stage of software development to prevent unauthorized access and protect sensitive data.

Question: How is user identity and access managed?

Security control:

Accreditations review are regularly performed.
A process allowing the deletion of accesses at the end of activity or when they are no longer necessary is implemented.
Administrator and privilege accounts use a strong authentication mechanism.
The principle of least privilege is implemented.
Access permissions are assigned according to the user's profile.

1.Security Audits
Periodic security audits are conducted to evaluate the effectiveness of our security infrastructure. These audits cover aspects such as network security, application security, and compliance with industry standards.

2. Access Control Evaluation
The accreditation reviews include a thorough examination of access control mechanisms to ensure alignment with security policies. This encompasses the verification of user roles, permissions, and adherence to the principle of least privilege.

3. Compliance Assessment
Our accreditation process incorporates a compliance assessment to verify adherence to relevant industry regulations and standards. This includes ensuring that our security practices align with established frameworks and guidelines.

4. Risk Management Analysis
A comprehensive analysis of risk management strategies is undertaken during accreditation reviews. This involves identifying potential risks, assessing their impact, and implementing mitigating measures.

5. Documentation Review
Accreditation reviews also involve a meticulous examination of documentation related to security policies, procedures, and incident response plans. This ensures that our practices are well-documented and up-to-date.

These regular accreditation reviews are essential for maintaining the highest standards of security, identifying areas for improvement, and ensuring ongoing compliance with industry best practices. The outcomes of these reviews contribute to the continuous enhancement of our system's security posture.

A process allowing the deletion of accesses at the end of activity or when they are no longer necessary is implemented.

Within our system, access management is a pivotal aspect of ensuring security and operational efficiency. We offer two primary types of access:

1.Login Access

This type of access allows users to log in to the system and execute various actions.

At the conclusion of a user's activity or when access is deemed unnecessary, we implement a secure disabling of the login functionality. This ensures that while the user's data remains in the system, their ability to log in and perform actions is revoked.

2.Permission Access

Following successful login, users are granted specific permissions and roles that dictate the actions they can undertake within the system.

When it becomes necessary to curtail or revoke these permissions, we facilitate this through the systematic removal of roles or permissions associated with the user account.

Our role management system allows for seamless transitions, enabling the modification of roles and permissions as per changing requirements.

In essence, our access management framework is designed not only to grant access efficiently but also to retract access systematically, thereby maintaining a secure and well-regulated system environment. This approach ensures that our users' data integrity is preserved while mitigating potential security risks associated with unnecessary access.

Question: How are passwords managed?

Security control: Passwords are regularly updated for sensitive and privilege accounts.

Strong passwords are enforced.

In adherence to robust security practices, our system enforces stringent password requirements. When creating a user account, the password must adhere to a specific string pattern, comprising the following elements:

●Upper Case Letter Ensuring the inclusion of at least one uppercase letter.

●Lower Case Letter Mandating the presence of at least one lowercase letter.

●Digit Requiring the inclusion of at least one numeric digit.

●Special Character Enforcing the presence of at least one special character.

●Length The password must be a minimum of 8 characters in length.

To fortify this security measure, we conduct both frontend and backend validations during the user account creation process. Front-end validation ensures that users are prompted to enter passwords meeting the specified criteria in real-time. Simultaneously, backend validation serves as an additional layer of verification, guaranteeing that the entered password complies with the defined pattern before finalizing the account creation.

This approach not only aligns with industry best practices but also significantly enhances the overall security posture of our system by promoting the use of robust and diverse passwords.

Question: How is authentication to critical information systems ensured?

Security control: Strong authentication mechanisms are defined and implemented.

Strong authentication mechanisms are defined and implemented.

In our commitment to fortify security, we have instituted a robust authentication framework. Key elements of our approach include:

1. Two-Factor Authentication (2FA)

Our system is equipped with Two-Factor Authentication, an additional layer of security beyond the traditional username and password. Users have the flexibility to enable or disable this feature at their discretion.

2. Verification Time Window

When 2FA is enabled, users are required to complete the verification process within a defined two-minute window. This time-sensitive verification enhances the security of the authentication process.

3. Maximum Attempt Threshold

To safeguard against unauthorized access attempts, we have implemented a maximum number of login attempts. After three consecutive unsuccessful attempts, the system automatically imposes a temporary block on authentication. This proactive measure serves as a deterrent against brute force attacks.

Our multifaceted approach to authentication not only elevates the overall security posture but also provides users with the flexibility to manage their authentication preferences. By integrating time-sensitive verification and imposing limits on login attempts, we strive to strike a balance between security and user experience, ensuring a resilient and user-friendly authentication mechanism.

Administrator and privilege accounts use a strong authentication mechanism.

For users with administrative or managerial privileges, a stringent security protocol is mandated. Specifically, individuals in these roles are compelled to utilize a Two-Factor Authentication (2FA) mechanism. Importantly, the option to disable 2FA is not available for profiles holding such elevated privileges.

This deliberate restriction is implemented to fortify the security of accounts with heightened access levels. By enforcing 2FA for administrators and managerial role holders, we enhance the overall resilience of our authentication system and mitigate potential risks associated with unauthorized access. This measure aligns with industry best practices and underscores our commitment to safeguarding privileged accounts and sensitive information within the system.

Question: How is user identity and access managed?

Security control: A process for assigning privileged accounts is formalized.

The principle of least privilege is implemented.

Our system meticulously adheres to the principle of least privilege to ensure a secure and controlled access environment. Here's how this principle is implemented:

1. Predefined Roles and Permissions

The system features predefined roles, each carefully crafted with specific permissions tailored to the responsibilities associated with that role. This ensures that users are granted only the minimum access necessary to fulfill their designated functions.

2. Custom Role Creation

In addition to predefined roles, users have the capability to create custom roles. This flexibility allows organizations to align access permissions precisely with their unique operational requirements.

3. Granular Permission Assignment

Every action within the system is associated with a distinct permission. The Create, Read, Update, and Delete (CRUD) operations, fundamental to data management, have individual sets of permissions. This granularity enables precise control over the actions users can perform.

By employing these measures, we establish a fine-tuned access control framework. Users, whether assigned predefined roles or custom-created roles, operate with the minimum necessary privileges. This meticulous approach not only enhances security but also contributes to the overall efficiency of our system by limiting access to only what is essential for each user's responsibilities.

Access permissions are assigned according to the user's profile.

Access permissions within our system are intricately tailored to align with the distinct roles associated with each user profile. This is achieved through a meticulous process wherein:

1. User Profiles

Every user is assigned a specific profile, reflective of their organizational role and responsibilities.

2. Role Assignment

Within each user profile, roles are assigned based on the individual's position and functions within the organization. These roles encompass predefined sets of permissions corresponding to the tasks and operations associated with the given role.

3. Granular Access Control

Access permissions are finely tuned to be task-specific. Each role is equipped with a precise set of permissions, ensuring that users can only perform actions relevant to their designated responsibilities.

4. Flexibility with Customization

For organizations with unique operational needs, the system allows the creation of custom roles. This grants the flexibility to tailor access permissions even further, accommodating specific tasks or requirements.

By adhering to this approach, we maintain a dynamic and adaptive access control system. Users, through their assigned roles, benefit from a nuanced set of permissions that streamline their interactions with the system, fostering both security and operational efficiency.

Question: How is user identity and access managed?

Security control: A process for assigning privileged accounts is formalized.

Our process for assigning privileged accounts is formalized to ensure precision and accountability. This structured approach involves the following key steps:

1. Employee Assignment

During the onboarding process or organizational changes, employees are systematically assigned to specific entities such as the company, location, or department.

2. Role Assignment

Concurrently, within the employee management view, relevant roles are assigned based on the individual's responsibilities and functions within the organization. This ensures that each employee has a clearly defined set of privileges aligned with their role.

3. Company, Location, and Department Views

Access to employees and role assignment is facilitated through dedicated views for the company, location, and department. This hierarchical structure provides a comprehensive overview of the organization's personnel and allows for efficient management of access privileges.

4. Role-Based Access Control (RBAC)

The assignment of roles is governed by Role-Based Access Control principles. This approach enables the formalization of access permissions based on the principle of least privilege, ensuring that individuals only possess the privileges essential for their designated roles.

By integrating these measures, our formalized process for assigning privileged accounts ensures a systematic, auditable, and accountable approach to access management. This not only enhances security but also streamlines administrative processes related to user privileges and roles within the organization.

Question: How are passwords managed?

Security control: Strong passwords are enforced.

Passwords are regularly updated for sensitive and privileged accounts.

As part of our security protocol, passwords for sensitive and privileged accounts undergo regular updates to enhance overall system security. The process is as follows:

1. Scheduled Password Updates

Administrators and managerial accounts are prompted to update their account passwords at predefined intervals, specifically every three months. This routine ensures that passwords remain dynamic and resilient against potential security threats.

2. Notification System

Users with privileged accounts receive timely notifications prompting them to initiate the password update process. These notifications serve as proactive reminders to ensure compliance with security policies.

3. Temporary Login Disabling

To enforce timely password updates, login access for administrators and managers is temporarily disabled until the password is successfully updated. This measure adds an extra layer of security and underscores the importance of adhering to the password update schedule.

By implementing these practices, we prioritize the security of sensitive accounts and maintain a proactive stance against potential security vulnerabilities. This structured approach to password management aligns with industry best practices and ensures a robust defense mechanism against unauthorized access to privileged accounts.

Question: How are security events managed?

Security control: Security events are qualified with the interlocutors concerned.

Security events are qualified with the interlocutors concerned.

In our commitment to maintaining a vigilant security posture, security events are systematically qualified with the relevant stakeholders. This involves a structured process to ensure effective communication and response to security incidents. The key components of this process include:

1.Incident Qualification

Each security event undergoes a thorough qualification process to determine its nature, severity, and potential impact. This qualification process is designed to categorize incidents based on predefined criteria.

2.Identification of Interlocutors

Upon qualification, the appropriate interlocutors, including relevant security personnel, administrators, and stakeholders, are promptly identified. This ensures that the right individuals are informed and involved in the incident response process.

3.Communication Protocol

A well-defined communication protocol is established to notify the concerned interlocutors about the security event. This includes clear and concise notifications outlining the incident details, potential risks, and recommended actions.

4.Collaborative Response

Interlocutors collaborate in the response effort, bringing their expertise and insights to effectively address and mitigate the security event. This collaborative approach ensures a swift and coordinated response to minimize any potential impact.

5.Post-Incident Analysis

After the resolution of the security event, a post-incident analysis is conducted. This involves a review of the incident response process, identification of lessons learned, and implementation of improvements to enhance future incident handling.

By qualifying security events with the relevant interlocutors, we ensure a proactive and collaborative approach to incident response. This structured process enhances our ability to detect, respond to, and mitigate security incidents in a timely and effective manner.

Question: How are contracts signed with third parties?

Security control: A non-disclosure agreement (NDA) with third parties is signed as soon as necessary.

NON-DISCLOSURE TERMS FOR THIRD PARTY

This is an Agreement between CONNECT RESOURCES ("CONNECTHR") and the Third Party that has executed this Agreement by either installing, executing or using ConnectHR' s software and/or Cloud Services. This Agreement sets forth the terms and conditions that govern Services under this Agreement.

Owner's Confidential Information may only be utilized for purposes of evaluating a potential commercial transaction / using certain services between the parties ("Purpose"). "Owner" means ConnectHR and may be an ConnectHR. "Recipient" means Company and may be an Affiliate of Company.

1.Confidential Information. "Confidential Information" means any commercial, financial, marketing, business, technical or other data, know-how, or other information related to Owner or its business which is disclosed either: (a) in tangible form and is marked "confidential" or "proprietary", or (b) orally or visually, and is designated as confidential or proprietary at the time of or within ten (10) days following disclosure, or (c) relates to the pricing or other terms of any product or service offering of Owner or its suppliers or of any agreement or proposed arrangement between the parties, or (d) under the circumstances, a person exercising reasonable business judgment would understand to be confidential or proprietary. Notwithstanding anything to the contrary in these Non-Disclosure Terms, Recipient acknowledges and agrees that even if individual portions of information are publicly available or non-proprietary, the specific combination of information provided to Recipient shall be deemed confidential and proprietary. For clarification, Confidential Information of Owner shall include Confidential Information disclosed by its Affiliates and to Recipient's Affiliates.

2. Confidentiality. The Recipient agrees to:

- use the Owner's Confidential Information solely for the Purpose;
- use the same degree of care, but not less than a reasonable degree of care, in protecting the Owner's Confidential Information, to prevent unauthorized use or publication, as it uses to protect its own confidential information;
- not reverse engineer, disassemble or decompile the Owner's Confidential Information;
- not export any Confidential Information without the Owner's written consent; or
- not disclose to any third party or copy any of the Owner's Confidential

Information without the Owner's written consent, such consent not to be unreasonably withheld, except that Recipient may disclose Owner's Confidential Information to its and its Affiliates' employees, contractors or professional advisors PROVIDED: (a) said persons have a need to know for the Purpose; (b) Recipient remains liable for said persons' use of Owner's Confidential Information; and each individual is under binding obligations of confidentiality no less restrictive than these Non-Disclosure Terms.

1. Term. These Non-Disclosure Terms shall remain in effect until terminated by either party with thirty (30) days prior written notice; provided however, that Recipient's obligation to protect Owner's Confidential Information shall survive expiration or written termination of these Non-Disclosure Terms for three (3) years from the last disclosure, except where source code or other Confidential Information that qualifies as a trade secret under applicable law is disclosed in which case the obligation is perpetual.

2. Exclusions. These Non-Disclosure Terms do not apply to Confidential Information:

· Which was in the public domain at the time of its disclosure, or which becomes public domain property through no fault of the Recipient;

· Which was rightfully in the Recipient's possession prior to disclosure by the Owner;
· Which was rightfully disclosed to Recipient by a third party without restriction;
· which was independently developed by the Recipient without use of or reference to the Owner's Confidential Information; or
· Disclosure of which is required under law, PROVIDED the Owner is given prompt prior written notice of the need for disclosure.

3. Ownership. Full ownership of Confidential Information remains with the Owner. No license, express or implied, is granted other than to use the Confidential Information for the Purpose.

4. Return. Upon termination or expiration of these Non-Disclosure Terms or upon Owner's request, whichever is earlier, Recipient shall immediately return to the Owner all Confidential Information (including all copies thereof) or certify in writing that all Confidential Information (including all copies thereof) has been destroyed.

5. Equitable Relief. In the event of a breach, or threatened breach, of these Non-Disclosure Terms, the Owner may seek appropriate equitable relief, including injunction, in addition to whatever remedies it may have at law.

6. Warranty. The Owner warrants that it has the right to disclose the Confidential Information to the Recipient. All other warranties, whether express or implied, are disclaimed.

7. Independent Development. Nothing in these Non-Disclosure Terms prevents either party from independently developing competing software, products or systems, provided such development by Recipient is not based upon the Confidential Information received from the Owner.

8. Separate Agreements. In the event the Company has entered into a separate agreement (either directly with ConnectHR or an authorized ConnectHR reseller) for the ConnectHR product and services, the parties acknowledge and agree that such agreement (and not these Non-Disclosure Terms) will govern the parties' rights and obligations in connection with the provisioning, access and use of the ConnectHR product and services.

9. General. These Non-Disclosure Terms are the entire agreement between the parties and supersedes all prior agreements relating to the Purpose. Nothing in this agreement is intended to limit or restrict liability for fraudulent pre-contractual representation. The laws of the UAE govern these Non-Disclosure Terms. No waiver or modification of these Non-Disclosure Terms is binding without the prior written consent of the other party. Neither party is required to proceed with any proposed transaction contemplated in this relationship. If any part of these Non-Disclosure Terms is held invalid or unenforceable, the remaining parts are unaffected. Nothing in this agreement is intended to confer a benefit on any third party.

10. Affiliates. The term "Affiliate" shall mean any entity which directly or indirectly, through one or more intermediaries, controls, or is controlled by, or is under common control with that party, by way of majority voting stock ownership or the ability to otherwise direct or cause the direction of the management and policies of the party. In the event that Owner discloses Confidential Information to an Affiliate of Recipient pursuant to these Non-Disclosure Terms, Recipient represents and warrants to Owner that (i) such Affiliate is subject to confidentiality obligations no less stringent than the obligations set forth herein, (ii) such Affiliate is authorized to receive access to the Confidential Information, and (iii) Recipient will remain fully liable for its' Affiliate's breaches of these Non-Disclosure Terms.

Question: How are contracts signed with third parties?

Security control: Contracts include security requirements.

THIRD PARTY SUPPLIER SECURITY ANNEX ("TPSA")

Whenever Supplier stores, processes, or otherwise accesses Confidential Information, or develops/provides products/software that is used by ConnectHR or ConnectHR Customers, or can otherwise materially impact ConnectHR systems, supplier shall comply with the requirements of this TPSA and shall contractually require all of its sub-processors (including any subcontractor that is storing, using, or processing any Confidential Information in connection with Supplier's delivery of Supplies to ConnectHR) to comply with the requirements of this TPSA.

Definition:

a. "System" means: a device or network of devices, virtual or actual, software, services and other elements that connect to store or process Confidential Information, including, without limitation, Supplies.

b. "Cardholder Data" means: (i) with respect to a payment card, the account holder's name, account number, security codes, card validation code/value, service codes (i.e., the three or four digit number on the magnetic stripe that specifies acceptance requirements and limitations for a magnetic stripe read transaction), PIN or PIN block, valid to and from dates, and embedded data (including magnetic stripe data and EMV data); and (ii) information and data related to a payment card transaction that is identifiable with a specific account, regardless of whether or not a physical card is used in connection with such transaction.

c. "PCI Standards" means: the security standards for the protection of payment card information with which the payment card companies collectively or individually require merchants to comply, including, but not limited to the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time, and any other applicable payment card industry data security requirements for Cardholder Data that are currently prescribed by the PCI Security Standards Council and as may be updated from time to time during the term of the TPSA.

d. "Vulnerability" means: a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability.

PCI Compliance:

If Supplier has access to or will collect, access, use, store, process, dispose of or disclose Cardholder Data under this TPSA, Supplier shall at all times remain in compliance with the PCI Standards, including remaining aware at all times of changes to the PCI Standards and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI Standards, in each case, at Supplier's sole cost and expense.

Security Management:

Supplier shall adopt, implement, maintain and monitor a written information security program that contains administrative, technical and physical safeguards designed to maintain service availability, data integrity, confidentiality and privacy of Confidential Information, which program shall include:

a. Executive review and support of all security-related policies.

b. Periodic (but no less than annual) risk assessments of all assets relevant to ConnectHR.

c. Periodic review of security incidents, including determination of root cause and corrective action.

d. Periodic internal audit to measure the effectiveness of controls.

Security Standards:

Supplier shall adhere to at least one of the following industry recognized security standards: ISO/IEC 27001 – Information Security Management Systems, or ISO-IEC 27002 – Code of Practice for International Security Management, the COBIT standards, NIST, or the PCI Standards.

Certifications/Attestations:

Supplier is required to submit to ConnectHR all current and applicable ISO/BS certifications (e.g., ISO27001 and ISO22301), System Organizational Control Reports (e.g., SOC2) or other certifications and attestations when available, and no more than annually, depending on the frequency of such audits, by using the electronic means as provided by ConnectHR. Third Party shall secure any rights necessary for ConnectHR to share these certifications/attestations with ConnectHR customers for whom the Supplier processes information or provides any type of indirect or direct maintenance or support. ConnectHR is entitled to share such certifications or attestations with ConnectHR customers upon request.

Data Center Certifications/Attestations:

Supplier must be certified against ISO 27001, PCI and provide SOC1 and SOC2 Type 2 reports as a minimum for all data center services. If data center services are subcontracted by the Supplier, the Supplier must ensure their subcontractors are also in compliance with these minimum requirements.

Penetration Testing:

Supplier shall provide to ConnectHR summary results of penetration testing undertaken by the Supplier of any Service processing Confidential Information, upon request at Supplier's expense. Such testing shall occur no less frequently than once every twelve (12) months. If any such reports include any findings flagged as "critical," "high" or "medium" security risks (industry standards like Common Vulnerability Scoring System should be used for vulnerability rating), Supplier shall promptly fix such issues, undergo additional penetration testing, and provide a new report to ConnectHR without any issues flagged as such level security risks. ConnectHR is entitled to share these reports with ConnectHR customers for whom the Supplier processes information or provides any type of indirect or direct maintenance or support.

Security Incident:

Supplier shall maintain (internal or external) incident management and forensics capabilities, policies and procedures, including detailed security incident escalation procedures. In addition to the obligation to report a Personal Data Breach in the CDPA (if applicable), Supplier shall notify ConnectHR immediately (which in no event will be longer than twenty-four (24) hours) at https://www.connecthr.com/about/trust-center/security/incident-management.html whenever Supplier reasonably suspects that any Confidential Information or Systems have been accessed, acquired, used or disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose ("Incident"). Supplier acknowledges that this ConnectHR point of contact address covers multiple affiliates, including ConnectHR, and therefore agrees any such notices will contain a specific reference to "ConnectHR Data." In parallel with providing such notice, Supplier shall without delay investigate the Incident, take necessary steps to eliminate or contain the exposures that led to such Incident, and keep ConnectHR advised of the status of such Incident and all matters related thereto. Upon ConnectHR's request, the Supplier must also provide an audit log of events that tracks service activity impacting Confidential Information upon ConnectHR's request. Supplier further agrees to provide assistance, requested by ConnectHR and/or ConnectHR's designated representatives, in the furtherance of any investigation, correction and/or remediation of any such Incident, including any notification that ConnectHR may determine appropriate to send to users, employees, customers or other individuals impacted or potentially impacted and/or the provision of credit monitoring service to such individuals, if and to the extent credit monitoring is required by applicable law. To the extent permitted by applicable laws or regulations, Supplier shall not give notice to any regulatory authority, any individual or any Supplier of any actual or potential Incident without first consulting with and obtaining ConnectHR's written permission. ConnectHR reserves the right to (i) immediately suspend any Services until it has determined that the Incident no longer poses a security or reputational risk to it, and (ii) immediately conduct additional on-site security audits and reviews of information concerning Supplier's security architecture, Systems and procedures.

In the event of an Incident directly resulting from Supplier's failure to use industry standard security measures, including standard encryption protocols and the requirements set forth herein, Supplier shall be responsible for the cost of notification and, if applicable, credit monitoring as described above in this paragraph.

Human Resource Security:

Supplier shall take reasonable steps to ensure the reliability of all Supplier Personnel who have access to Confidential Information, including:

Background Checks:

Supplier shall require all Supplier Personnel who will have access to Confidential Information to undergo and satisfy the requirements of a reasonable background investigation that Supplier conducts or causes to be conducted at its expense that is designed to confirm that none of

such persons pose a threat to the safeguarding of Confidential Information or other Confidential Information or a threat to the integrity of the business operations of ConnectHR or any of its customers. In executing its pre-hire screenings, Supplier is responsible for conducting its background checks and decisions in accordance with applicable laws. At a minimum (and at all times in accordance with applicable laws which may impose greater or different requirements), in order to be reasonable hereunder, background checks must include the following:

b. Adherence to Security Policy. Supplier shall require all Supplier Personnel to acknowledge in writing, at the time of hire and annually thereafter, to adhere to Supplier's security policy and to protect all Confidential Information at all times, consistent with provisions of this Exhibit. Such policy must be according to industry-accepted standards.

c. Security and Privacy Awareness Training. Supplier shall require all Supplier Personnel to undergo security and privacy awareness training at the time of hire and annually thereafter.

d. Disciplinary Policy and Process. Supplier shall maintain a disciplinary policy and process, to be used when Supplier Personnel violate Supplier security policy or access Confidential Information without prior authorization.

Access Management:

Supplier shall use formal access management processes for the request, review, approval, and provisioning of all Supplier Personnel with access to any System. Access management controls will include:

a. Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes.

b. Unique identifiers (user IDs) are required for access to all Confidential Information or Systems. Procedures are in place so that requested user accounts and authorization changes are implemented only in accordance with approved policies and procedures that are based on industry best practices (for example, no rights are granted without authorization).

c. In case Supplier Personnel leaves the company, their access rights are revoked within 24 hours. When Supplier Personnel change their assigned role within the company, their access rights are timely revoked or adapted. Supplier has a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, Systems force a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver

d. Display screens for all systems that could disclose information allowing access to another Supplier's device or system or screens used to handle Confidential Information should be positioned so that unauthorized persons cannot readily view them through a window, over a shoulder, or by similar means.

e. Mobile devices that could provide access to devices or systems where Confidential Information is stored must be kept in the possession of Supplier Personnel or locked in a secure location when not in use. Mobile devices must not be checked in as luggage when travelling.

Malware Control:

Supplier shall maintain effective malware controls, including:

a. All Systems, all supporting Supplier systems, and all laptop computers, desktop computers, and mobile devices that access Systems will include commercial-grade anti-virus, anti-malware, anti-spyware controls that include real-time scanning, periodic whole-system scanning, and regular updates. This includes signature or behavior-based detections of malware, viruses, spyware and trojans as it applies to ingress and egress points such as email services and file transfers. It also mitigates security risks for malicious code on systems, endpoints, and devices.

b. Supplier shall utilize spam-filtering systems to block incoming messages containing spam and malware.

c. Supplier shall utilize web-filtering systems to block access to Internet web sites containing or suspected to contain malware.

d. Supplier shall utilize commercial-grade firewalls that restrict all inbound and outbound traffic except for those specific ports and IP addresses necessary to perform the Service. Supplier continuously and actively detects systems and infrastructure against attacks through operation of an enterprise threat detection system and additional tools, including using and analyzing audit logs.

Intrusion Detection/ Intrusion Prevention:

Supplier shall maintain network-based intrusion detection/ intrusion prevention system(s) to detect and prevent unwanted or hostile network traffic. Upon the availability of updates by the software provider, Supplier shall update its intrusion detection/prevention software promptly and without delay.

Data Encryption:

Data cannot be read or modified without authorization during transfer and at rest. Supplier shall use current commercial industry standard secure encryption methods to protect Confidential Information, including the following:

a. Encryption of Transmitted Data. Supplier shall use current Internet-industry standard secure encryption methods designed to encrypt communications during transit between its server(s) /

service(s) and ConnectHR browser(s) and between all its servers and all ConnectHR's server(s) / service(s) / end-points. This applies to both physical and network-based data transfer. Data in transfer within secured networks and networks in control of Supplier is appropriately secured.

b. Encryption of Stored Data. Supplier shall use Internet-industry standard secure encryption methods to encrypt data at rest, including on mobile devices such as laptop computers, designed to protect stored Confidential Information.

Supplier shall store Confidential Information only on server(s) that are segregated from servers accessed from the Internet by other users of Supplier Supplies. Mobile devices that could provide access to devices or Systems where Confidential Information is stored use Supplier controlled network encryption when connecting to Supplier networks remotely.

c. Encryption Key Management. Supplier shall have a defined key management policy that defines encryption key requirements, rotation, and lifecycle, including creation, distribution, revocation, archival, and destruction.

System Hardening:

Supplier shall use Internet-industry standard system and device hardening standards for all Systems that store, process, or transmit Confidential Information. Such hardening standards will include:

a. Disable or remove all unnecessary services.

b. Security patch management is implemented to provide regular and periodic deployment of relevant security updates.

c. Change all default passwords.

d. Rename administrative user accounts.

e. Each server performs only one function (e.g., web server, application server, and database server should occupy separate systems).

f. Employ host-based intrusion detection and prevention mechanism.

g. Passwords are stored using industry accepted hashing algorithm; only administrators that support the function have access to stored hashes, when necessary.

Business Continuity:

Supplier will ensure to monitor and document the reliability, maintainability, serviceability and availability of a system or service on a continuous basis. The Supplier shall conduct at least annual testing of the Supplier's Business Continuity Plan and provide a copy of the Business Continuity Plan and the results of the test to CONNECTHR upon request.

Stipulation of Availability:

Supplier should ensure minimum availability of 99.99% per month, unless otherwise agreed upon in the relevant Statement of Work (SOW). Supplier will ensure Denial-of-Service (DoS) preventive measures are in place for the data center providing the service.

Vulnerability Management.

a. Infrastructure Scans. Supplier shall perform periodic (but no less than once per month) vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities shall be remediated on a risk basis. Supplier shall install all Medium, High, and Critical security patches for all components in its production and development environment as soon as commercially possible.

b.Application Scans. Supplier shall perform periodic (but no less than once per quarter, as well as after making any change to the Supplier System application vulnerability scans). Vulnerabilities shall be remediated on a risk basis. Supplier shall install all Medium, High, and Critical security patches for all components in its production and development environment as soon as commercially possible.

c.External Application Testing. Supplier shall perform security code reviews, including both static testing and dynamic testing whenever changes occur to source code, or when new code is deployed.

d.Vulnerability Notification. Supplier shall notify CONNECTHR of a confirmed Vulnerability without undue delay by sending notice of it to: vas@ConnectHR.com. The notice must include (I) a description of the Vulnerability, (II) impacted products or systems including the applicable versions, and (III) information reporting to the National Institute of Standards and Technology's Common Vulnerabilities and Exposures Program, including the CVE-ID, if applicable.

Data Management:

a. Storage of Information. Supplier shall store Confidential Information (to the extent permitted by the terms herein) only on servers controlled by Supplier and/or its third-party hosting provider. End user workstations, laptops, USB devices, CD-ROM, DVD-ROM, and mobile devices shall not be used to store any Confidential Information.

b. Segregation of Data. Supplier shall use physical and logical controls to segregate Confidential Information from that of other customers. Supplier shall produce documentation describing data segregation controls to CONNECTHR upon request.

c. Backups. Supplier shall protect Confidential Information against loss, backup copies of information, software and system images shall be taken and tested regularly.

d. Change of the Hosting Provider. Supplier shall notify CONNECTHR at least 90 days in advance before changing or adding a hosting provider for Data or System deployment and such notice will identify the selected hosting provider (or provider options under consideration by Supplier). Supplier shall provide information as reasonably requested by CONNECTHR about the security practices and procedures of the selected provider, including its physical security

controls and environment. In the event CONNECTHR reasonably determines that the security practices and physical security of the new provider are not sufficient or comparable to those employed by the hosting provider previously used by Supplier, CONNECTHR may terminate an Order with written notice of at least fifteen (15) days.

e. Change of Supplier (Fourth Party) Subcontractors. Supplier shall notify CONNECTHR at least 90 days in advance before changing subcontractors that will have access to Confidential Information or System that transmit, store, or process Confidential Information. Supplier shall provide to CONNECTHR on request any due diligence that was conducted to determine the subcontractor's suitability for performing or delivering Supplies supporting CONNECTHR or CONNECTHR customers. CONNECTHR reserves the right of termination, both for Supplier's breach of security practice standards, or for violation of the 90-day limit.

f. Change of Supplier Processes. Supplier shall notify CONNECTHR of any major changes to processes the Supplier uses to support CONNECTHR or CONNECTHR customers at least 30 days in advance.

g. Return/Destruction of Data. As between CONNECTHR and Supplier, all Confidential Information and data carriers and any copies, reproductions, summaries, analyses or extracts thereof or based thereon, including (without limitation) those made by Supplier in performance or delivery of the Supplies, are the property of CONNECTHR (including all customer and Supplier data CONNECTHR is responsible for) and shall be promptly returned via CONNECTHR approved methods to CONNECTHR upon any of the following events, whichever is earliest: (i) upon CONNECTHR's request; or (ii) upon completion of Supplies; or (iii) upon expiry or termination of any agreement under which Supplies are delivered. Alternatively, where Confidential Information and/or data carriers cannot be returned, or if CONNECTHR elects so, Supplier shall destroy and certify to CONNECTHR in writing that it has permanently destroyed all Confidential Information in its possession or control and data carriers which otherwise would have to be returned in accordance with this Section 16(d). The written certificate of destruction shall detail the destruction method used to permanently destroy all Confidential Information and/or data carriers, the date of destruction and individual who performed the destruction. Supplier's destruction of Confidential Information under this Section shall be in compliance with industry standard practices.

h. Supplier shall not access, use, store, transfer, or disclose any Confidential Information, except as necessary to perform or deliver the Supplies.

Security Logs:

Supplier shall employ procedures that all systems, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized logging system in order to enable the security audits referred to below. Additionally, Supplier shall employ the following procedures:

a. Logs shall be retained for at least one (1) year.

b. Logs shall not contain Confidential Information.

c. Logs shall be protected from unauthorized modification or erasure.

d. Logs shall be backed up on a daily basis.

e. Logs shall be monitored for risk and functional anomalies.

Secure Remote Access:

Supplier shall employ two-factor authentication for all remote access to internal and confidential information and systems.

Data Retention:

Data will be securely retained for the time requirements and in the manner in accordance with privacy and regulatory laws for the region of demographic persons that the Supplier creates, stores, or processes. This may continue after the primary engagement or project is closed.

Issue Remediation Supplier agrees to work with CONNECTHR and their designees to remediate issues or risks identified through assessments, conducted on behalf of CONNECTHR or conducted on behalf of the Supplier. Supplier shall remediate at its cost those issues identified as high within 30 days, those identified as Medium or low within 90 days, provided that an issue is within the reasonable control of the Supplier.

Secure Development:

Supplier ensures that all Supplies developed by for the Supplier to provision Supplies have been developed following a secure software development lifecycle process which includes industry best practices for achieving and sustaining required security qualities for confidentiality, integrity and availability protection. In addition, software security vulnerabilities (see, for example the OWASP Top Ten or CWE listings) shall be avoided. The expected security measures and controls applied for software provisioning, such as Security Education of the development workforce, Secure Architecture and Design principles, Secure Coding practices, Security Testing methods and tools applied, Security Response to react timely on applicable software vulnerabilities that become known, as well as application security controls embedded and enforced by the software itself, such as identity

management, authentication, authorization, encryption etc. shall be adequate to meet relevant business, technology and regulatory risks according to international standards such as ISO/IEC 27034. The Supplier has procedures in place to ensure integrity of software updates and can demonstrate that precautions are taken to ensure that any own or Supplier or open source software used for providing the Supplier Supplies do not contain known backdoors, viruses, trojans or other kind of malicious code.

Security Audits by CONNECTHR:

CONNECTHR is entitled to carry out security audits on the systems, security processes and procedures of the Supplier at least once per year and any time upon prior notification in the case of a request from an external authority, reasonable suspicion of a security incident or findings in documented security audits or other documentation provided to CONNECTHR. Should a security scan of Supplier's resources containing Confidential Information be required to identify or validate deficiencies, CONNECTHR shall identify the tools used for testing and the methods used. CONNECTHR and the Supplier shall mutually agree to the scope, approach and

timing of such testing so that scanning does not interfere with Supplier's normal business operations and performance. Audit results shall contain only relevant information for the Supplies provided to CONNECTHR. If security vulnerabilities are discovered during the check, the Supplier shall take reasonable steps to mitigate the security vulnerabilities and to minimize any damage from the security incident.

Regulatory and Legal requirements:

Under the applicable regulations and laws, CONNECTHR and its customers are required to execute enhanced audit, disaster recovery (including backups) and other data protection requirements, current or in the future, whether directly or in support of customer's obligations. Accordingly, Supplier will:

a. Allow regulator or customer on-site audit rights to the extent required by law.

b. Provide responses to questionnaires to the extent specific responses are required by applicable regulations and laws.

c. Allow for customer termination rights for any deficiencies or noncompliance with this agreement or any applicable regulation or laws that requires such right under the applicable circumstances.

CONNECTHR Supplier Risk Management (TPRM) Process:

Supplier is required to undergo and complete the CONNECTHR TPRM process. In addition, Section "Issue Remediation" will apply for issue remediation. CONNECTHR reserves the right of service termination in both cases, if either the CONNECTHR TPRM Process or the issue remediation is not completed.