BUSINESS PROCESSES AND SECURITY POLICY

CYBERTECH CORPORATION

POLICY: HUMAN RESOURCES INFORMATION SECURITY STANDARDS

March 17, 2024

Student ID	Student Name
100952215	Mehul Patel
100956102	Boby Anna John
100955867	John Joshy Francis
100950933	Niharkumar Jadav
100344918	Jaison Bhatti

1. TABLE OF CONTENTS

2. REVISION HISTORY

Version	Title	Author	Issue Date	Classification	Changes
1.0	Human Resource Security Policy	Mehul Patel John Joshy Francis Boby John Niharkumar Jadav Jaison Bhatti	March 17, 2024	CONFIDENTIAL	Creation

2.1 REFERENCE

This policy was created using the ISO 27001:2013 as the reference.

3. POLICY OVERVIEW

This section describes the purpose and scope of the Human Resource Security Policy.

3.1 PURPOSE

- The objective of Cybertech Corporation's Human Resources Security framework is to establish and maintain robust measures aimed at safeguarding the confidentiality, integrity, and availability of information. By implementing comprehensive policies and procedures, we seek to mitigate risks associated with unauthorized access, disclosure, or misuse of sensitive data, thereby ensuring the trust and confidence of our clients, stakeholders, and partners.

3.2 SCOPE

- This framework applies to all individuals associated with Cybertech Corporation, including employees, contractors, and third-party vendors. It encompasses personnel at all levels and across all departments, acknowledging the collective responsibility in upholding information security standards and fostering a culture of vigilance and accountability throughout the organization.

4. POLICY STATEMENT

The following sections will present the policy statement in 5 sections broken down into 11 main aspects:

Prior to Employment

Screening

Terms and Conditions of Employment

During Employment

Management Responsibilities

Information security awareness, education, and training

Disciplinary Process

Termination and Change of Employment

Termination or Change of Employment Responsibilities

Managing Third-Party Risks

Vendor Evaluation

Contractual Agreements

Ongoing Monitoring

Incident Management and Response

Incident Response Plan

Employee Involvement

4.1 PRIOR TO EMPLOYMENT

- Before employment, it is imperative for the Council to adhere to its established recruitment guidelines or policy, such as the Recruitment and Selection Policy, to ensure that potential users are recruited for roles in line with organizational standards. This approach not only ensures alignment with corporate requirements but also mitigates the risk of theft, fraud, or misuse of information or information systems by those users. In cases where it is applicable, local authorities may consider providing a checklist outlining the necessary actions to be followed when new users are hired by the Council or when existing staff members require access to information or information systems.

4.1.1 SCREENING

- Cybertech Corporation will conduct thorough background checks on all prospective employees and third-party personnel in accordance with relevant laws, regulations, and industry standards. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved.
- The basic requirements for Council employment must be,
  - Minimum of two satisfactory references.
  - Completeness and accuracy check of employee's application form.
  - Confirmation of claimed academic and professional qualifications.
  - Identity check against a passport or equivalent document that contains a photograph.
- Background checks will verify the credibility of candidates and contractors, including criminal history, employment history, educational credentials, and references.
- The following requirements **must** be met:
  - Minimum of 2 satisfactory references.
  - Completeness and accuracy check of employee's application form.
  - Confirmation of claimed academic and professional qualifications.
  - Identity check against a passport or equivalent document that contains a photograph. Identity must be proven through visibility of:
    - A full 10 year passport.
  - Or two from the following list:
    - Driving licence.
    - Birth certificate.

        - Proof of residence – i.e. council tax or utility bill.
    - Verification of full employment history for the past 3 years.
    - Verification of nationality and immigration status.
    - Verification of criminal record (unspent convictions only).
- Criminal Records Bureau checks on the user must be carried out to an appropriate level as demanded by law.
- Additional screening measures, such as credit checks and security clearance verification, may be conducted for positions requiring access to particularly sensitive information or systems.
- All the above requirements for verification checks must be applied to technical support and temporary staff that have access to those systems or any copies of the contents of those systems (e.g. backup tapes, printouts, test data-sets).

4.1.2 Terms and Conditions of Employment

- As part of their contractual obligation users must agree and sign the terms of their employment contract, which shall state their and the Council's responsibilities for information security. This must be drafted by the Council's lawyers and must form an integral part of the contract of employment.
- The terms and conditions of employment for all employees and contractors will explicitly outline their responsibilities regarding information security. Employees and contractors will be made aware of the consequences of security policy violations, which may include disciplinary action, termination of employment, legal consequences, and financial liabilities.
- Security policy agreements will be incorporated into contractual agreements, ensuring that all parties understand and acknowledge their obligations to adhere to Cybertech Corporation's information security policies and standards
- Each user must sign a confidentiality statement [or equivalent] that they understand the nature of the information they access, that they will not use the information for unauthorised purposes and that they will return or destroy any information or assets when their employment terminates.

4.2 DURING EMPLOYMENT

4.2.1 MANAGEMENT RESPONSIBILITIES

PROCESS AND PROCEDURE ADHERENCE

- The objective of this policy is to establish guidelines for ensuring strict adherence to security processes and procedures across all departments and personnel within Cybertech Corporation.
- Protocol Enforcement
  - *Secure Handling Protocols*: Employees are required to adhere to established protocols for securely managing client records and corporate data.
  - *Encryption Usage*: Data encryption must be employed for transmitting and storing sensitive information to prevent unauthorized access.
  - *Access Controls*: Implementing and enforcing access controls to restrict access to sensitive systems and data on a need-to-know basis.
  - *Data Classification*: Adhering to data classification policies to categorize information based on its sensitivity and apply appropriate security controls.
- Monitoring and Compliance
  - *Regular Audits*: Conducting periodic audits and compliance checks to monitor adherence to security policies and identify any deviations or areas for improvement.
  - *Corrective Actions*: Implementing corrective actions and remediation measures to address non-compliance issues promptly and prevent recurrence.
  - *Documentation*: Maintaining comprehensive documentation of security processes, procedures, and audit findings for accountability and transparency.
- Employee Accountability
  - *Accountability Measures*: Holding employees accountable for their actions and responsibilities related to security processes and procedures.
  - *Training and Awareness*: Providing ongoing training and awareness programs to ensure employees understand their obligations and the importance of compliance.

ROLES AND RESPONSIBILITIES

- Job descriptions and contracts will clearly define security roles and responsibilities for all positions within Cybertech Corporation.
- This includes specific duties related to information security, such as data handling procedures, access control responsibilities, and compliance with security policies and standards. Managers and supervisors will be responsible for ensuring that employees understand their security-related duties and are adequately trained to fulfil them.
- Determining the appropriate level of access to information or information systems for each user will fall under the purview of the Information Asset Owner. For detailed guidelines, please refer to the designated Information Protection Policy, which will provide comprehensive instructions regarding access management.
- Line managers, or their equivalents, will be tasked with promptly notifying the IT Helpdesk or the relevant department about the creation, modification, or termination of user accounts, following a predefined process.
- The information security responsibilities of users must be defined and documented and incorporated into induction processes and contracts of employment. As a minimum this will include
    - A statement that every user is aware of, and understands, the following Council policies
        - Information Protection Policy [or equivalent].
        - Email Policy [or equivalent].
        - Internet Acceptable Usage Policy [or equivalent].
        - Software Policy [or equivalent].
        - IT Access Policy [or equivalent].
        - Information Security Incident Management Policy [or equivalent].

ACCESS CONTROL

- Principle of Least Privilege
    - Access rights will be granted based on the principle of least privilege, ensuring that individuals only have access to the information and systems necessary to perform their duties.

- *Job Requirements*: Access permissions will be aligned with job requirements to minimize the risk of unauthorized access.

- Authentication and Authorization Mechanisms
  - *Secure Authentication*: Implementing secure authentication mechanisms, such as multi-factor authentication (MFA), to verify the identity of users before granting access.
  - *Role-Based Access Controls (RBAC)*: Utilizing RBAC to assign access permissions based on the roles and responsibilities of individuals within the organization, further limiting access to sensitive resources.

OPERATIONAL SECURITY:

- Prevention of Unauthorized Software Installations
  - Measures will be implemented to prevent unauthorized software installations on corporate systems, reducing the risk of introducing malicious software.
  - Administrative Controls: Administrative controls will be established to restrict users' ability to install software without proper authorization.
- Ensuring System Integrity
  - *Integrity Measures*: Measures will be implemented to ensure the integrity of corporate systems, preventing unauthorized modifications or tampering.
  - *Secure Data Handling*: Secure data handling procedures will be enforced to maintain the confidentiality and integrity of sensitive information.
- Secure Data Transfer
  - *Encryption and Secure Protocols*: Secure encryption methods and protocols will be employed to protect sensitive information during transmission, both within the organization and over external networks.
  - *Education and Awareness*: Employees will be educated on the risks associated with unauthorized software installations and instructed to report any suspicious activity or security concerns to the appropriate authorities.

4.2.2 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

- The objective of this policy is to ensure that all employees, contractors, and third-party personnel receive comprehensive security awareness training to mitigate risks and enhance the security posture of Cybertech Corporation.
- *Tailored Training*: Training sessions will be tailored to the specific roles and responsibilities of individuals within the organization.
- *Content Coverage*: Training content will encompass a wide range of topics, including but not limited to:
  - *Phishing Awareness*: Recognizing and reporting phishing attempts and other social engineering tactics.
  - *Password Hygiene*: Best practices for creating and managing secure passwords and multi-factor authentication (MFA) usage.
  - *Secure Data Handling*: Protocols for handling and protecting sensitive client information and corporate data.
  - *Incident Response*: Procedures for identifying, reporting, and responding to security incidents promptly and effectively.
  - *Regulatory Compliance*: Understanding and adhering to relevant regulatory requirements and industry standards.
- Delivery Methods
  - *Instructor-led Sessions*: Conducting in-person or virtual instructor-led training sessions for interactive learning experiences.
  - *Online Modules*: Providing access to self-paced online training modules through a learning management system (LMS) for flexibility and accessibility.
- Frequency
  - Training sessions will be conducted regularly, with refresher courses provided annually or as needed to reinforce key concepts and address emerging threats.

4.2.3 DISCIPLINARY PROCESS

DISCIPLINARY PROCESSES

- Establishment of Clear Processes
  - The purpose of establishing clear processes for addressing security breaches is to ensure a consistent and effective response to incidents within the organization.
  - *Incident Reporting*: Employees must report any security breaches or suspicious activities to the designated authority or IT security team promptly.
  - *Investigation*: Upon receiving a report, the IT security team will conduct a thorough investigation to assess the nature and extent of the security breach.
  - *Documentation*: All steps taken during the investigation process will be documented, including evidence collected, findings, and actions taken.
  - *Response Plan*: Based on the investigation findings, the IT security team will develop and implement a response plan to mitigate the impact of the security breach and prevent further damage.
  - *Communication*: Clear and timely communication will be maintained with relevant stakeholders throughout the incident response process, ensuring transparency and accountability.
- Potential Disciplinary Actions
  - The purpose of defining potential disciplinary actions is to deter employees from engaging in behaviour that violates security policies and to ensure accountability for such actions.
- Defined Actions:
  - *Verbal Warning*: A verbal warning may be issued for minor violations or first-time offenses, serving as a reminder of the organization's security policies and expectations.
  - *Written Warning*: A written warning may be issued for repeated violations or more serious offenses, documenting the incident, and outlining consequences for future breaches.
  - *Suspension*: In cases of severe or repeated violations, employees may face suspension from work for a specified period, reflecting the seriousness of the breach and providing an opportunity for reflection.

- *Termination*: Persistent or egregious violations of security policies may result in termination of employment, emphasizing the organization's commitment to maintaining a secure work environment.

4.3 TERMINATION AND CHANGE OF EMPLOYMENT

4.3.1 TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES

ROLE CHANGES

- Access Rights Review
  - The purpose of the Access Rights Review is to ensure that employees have appropriate access permissions aligned with their new responsibilities when they change roles within the organization.
  - *Identification*: Upon notification of a role change, the IT department will identify the affected employee's existing access rights and compare them with the access requirements of the new role.
  - *Review and Adjustment*: Access rights will be reviewed by the IT department or designated personnel to determine if any adjustments are necessary to align with the employee's new responsibilities.
  - *Authorization*: Adjustments to access rights will be authorized by the employee's manager or supervisor, ensuring that changes are in line with business requirements and security principles.
  - *Documentation*: All changes to access rights will be documented, including the rationale for adjustments and the authorization process followed.
- Training and Awareness
  - The purpose of Training and Awareness programs is to provide employees transitioning to new roles with the necessary knowledge and understanding of their security responsibilities and associated risks.
- Program Content
  - *Role-specific Training*: Employees will receive role-specific training tailored to their new responsibilities, focusing on information security policies, procedures, and best practices relevant to their role.
  - *Risk Awareness*: Training programs will include components on risk awareness, highlighting potential security risks associated with their new role and strategies for mitigating these risks.

- *Handling Sensitive Information*: Employees will be educated on the proper handling of sensitive information relevant to their role, emphasizing confidentiality, integrity, and availability principles.
- *Incident Response*: Training will cover incident response procedures, ensuring that employees understand their role and responsibilities in responding to security incidents and reporting any suspicious activity.

TERMINATION - EXIT PROCESSES

- The purpose of defining and enforcing exit processes is to ensure the secure and orderly transition of employees upon termination or role change, safeguarding sensitive information and company assets.
- *Access Rights Revocation*: Upon termination or role change, access rights to information systems, facilities, and company resources will be promptly revoked to prevent unauthorized access and protect against potential misuse.
- *Asset Return*: Employees departing from the company will be required to return all company-owned assets, including electronic devices, access badges, keys, and any other equipment provided for work-related purposes. A formal checklist may be utilized to document the return of assets.
- *Confidentiality Agreements*: Employees will be reminded of their ongoing obligations regarding confidentiality and data protection, emphasizing the importance of maintaining confidentiality even after termination or role change.

AWARENESS OF POST-EMPLOYMENT OBLIGATIONS

- The purpose of reminding employees of their post-employment obligations is to reinforce their awareness of confidentiality and data protection requirements, mitigating the risk of unauthorized disclosure or misuse of sensitive information.
- *Communication*: Prior to departure, employees will receive reminders and guidance regarding their post-employment obligations related to confidentiality and data protection. This communication may take the form of email notifications, exit interviews, or written documentation provided during the offboarding process.
- *Training and Education*: Employees will have access to resources and training materials that highlight their ongoing responsibilities regarding the protection of company information and intellectual property. This may include refresher courses on data handling policies, nondisclosure agreements, and relevant legal obligations.

- *Acknowledgement*: Employees will be required to acknowledge their understanding of post-employment obligations through a formal acknowledgment process, affirming their commitment to upholding confidentiality and data protection principles even after leaving the company.

4.4 MANAGING THIRD-PARTY RISKS

4.4.1 VENDOR EVALUATION

- The purpose of vendor evaluation is to assess the security practices and capabilities of third-party vendors to ensure they align with Cybertech Corporation's security requirements and standards.
    - *Security Assessment*: Prior to engaging with third-party vendors, Cybertech will conduct comprehensive security assessments to evaluate their security posture, including their information security policies, procedures, controls, and incident response capabilities.
    - *Compliance Review*: Vendors will be evaluated against established security criteria, which may include adherence to industry standards (e.g., ISO/IEC 27001), regulatory requirements, and specific security controls mandated by Cybertech.
    - *Risk Analysis*: A risk analysis will be conducted to identify and assess potential security risks associated with engaging third-party vendors, considering factors such as the sensitivity of data involved, the criticality of services provided, and the vendor's access to Cybertech's systems and information.

4.4.2 CONTRACTUAL AGREEMENTS

- The purpose of contractual agreements is to formalize security expectations, incident reporting procedures, and data handling requirements with third-party vendors, establishing clear obligations and responsibilities to protect Cybertech's interests.
- Elements:
    - *Security Expectations*: Contractual agreements will specify the security expectations and standards that vendors must adhere to, including requirements for data protection, access controls, encryption, and cybersecurity incident management.
    - *Incident Reporting*: Vendors will be required to promptly report any security incidents or breaches affecting Cybertech's systems or data, enabling timely response and mitigation measures to be implemented.

- *Data Handling Procedures*: Contractual agreements will outline specific data handling procedures and restrictions, detailing how sensitive information should be handled, processed, stored, and transmitted by the vendor.

4.4.3 ONGOING MONITORING

- The purpose of ongoing monitoring is to ensure that third-party vendors continue to meet Cybertech's security requirements and maintain compliance with established standards throughout the duration of their engagement.
- Approach:
  - *Regular Reviews*: Cybertech will conduct regular reviews of third-party vendor performance and adherence to security requirements, including scheduled assessments, audits, or performance evaluations.
  - *Compliance Checks*: Ongoing monitoring activities will include periodic compliance checks to verify that vendors are implementing agreed-upon security measures and addressing any identified deficiencies promptly.
  - *Performance Metrics*: Key performance metrics related to security, such as incident response times, compliance status, and adherence to service level agreements, will be monitored to assess vendor performance and identify areas for improvement.

4.5 INCIDENT MANAGEMENT AND RESPONSE

- The Incident Management and Response Policy aims to establish a framework for effectively detecting, responding to, and mitigating security incidents within Cybertech Corporation. By implementing this policy, Cybertech seeks to minimize the impact of security breaches, protect sensitive data, and maintain the continuity of its business operations.

4.5.1 INCIDENT RESPONSE PLAN

- Development and Implementation:
  - Cybertech Corporation has developed and maintains a comprehensive Incident Response Plan (IRP) to guide its response to security incidents.
  - The IRP outlines predefined procedures for detecting, containing, and mitigating security issues, ensuring swift and coordinated action to minimize the impact on the organization and its stakeholders.
- Key components of the IRP include:
  - *Incident Detection*: Procedures for identifying potential security incidents through monitoring, logging, and threat intelligence.
  - *Containment and Mitigation*: Steps to isolate affected systems, limit the spread of the incident, and implement measures to mitigate further damage.
  - *Evidence Preservation*: Protocols for preserving evidence related to the incident, ensuring its integrity for investigation and legal purposes.
  - *Communication and Reporting*: Guidelines for communicating with relevant stakeholders, including internal teams, regulatory authorities, and affected parties, and reporting the incident in accordance with legal requirements.
  - *Recovery and Resumption*: Processes for restoring affected systems and services to normal operations while minimizing downtime and disruption.

4.5.2 EMPLOYEE INVOLVEMENT

- Cybertech prioritizes employee education and awareness to empower staff in recognizing and reporting security events and vulnerabilities.

- All employees, independent contractors, and third-party suppliers receive comprehensive training on security risks, including malware infections, phishing scams, and unauthorized access attempts.
- Training programs emphasize the importance of promptly reporting incidents through approved channels and raising security concerns when necessary.
- By engaging its workforce as active participants in the incident response process, Cybertech enhances its overall security posture and resilience against emerging threats.