BUSINESS PROCESSES AND SECURITY POLICY

CYBERTECH CORPORATION
POLICY: PHYSICAL AND ENVIRONMENTAL SECURITY

March 31, 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	Physical and Environmental Security Policy	Mehul Patel	March 27, 2024	PUBLIC	Creation
1.1		John Joshy Francis	March 28, 2024	PUBLIC	QA
1.2		Boby John	March 29, 2024	PUBLIC	Update
1.3		Niharkumar Jadav	March 30, 2024	PUBLIC	Update
1.4		Jaison Bhatti	March 31, 2024	PUBLIC	Update

3. APPROVAL

Name	Title	Date	Approved
Ahmad Barakat	Professor of MGMT1100	March 31, 2024	YES

4. REFERENCE

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

3. POLICY OVERVIEW

3.1 PURPOSE

The purpose of the Physical and Environmental Security Policy is to stop illegal direct entry, harm, and disruption to the company's data and data process infrastructure, prevent loss, damage, theft or compromise of assets and interruption to the organization's operations

3.2 SCOPE

The policy statements written in this document are applicable to all resources at Cybertech Corporation and at all levels of sensitivity such as:

- All full-time, part-time and temporary employees staffed by Cybertech Corporation.
- Contractors and consultants who are working on behalf of Cybertech Corporation.
- Any individual or third-party groups who have been granted access to Cybertech Corporations’s internal systems and information.

3.3 TERMS AND DEFINITIONS

Terms	Definition
Asset	Any item of value to the organization that needs to be protected, including information, software
Authentication	Process of verifying the identity of a user
Authorization	Granting of rights to a user, group, or system to access data or resources
Background Check	Process of verifying the legal, financial, and personal character of an employee or potential employee
Compliance	Adhering to laws, regulations, guidelines, and specifications relevant to the organization
Data Protection	Measures and processes for ensuring the privacy and protection of personal data
Encryption	Process of converting information or data into a code to prevent unauthorized access
Firewall	Network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules
Incident	Event that has the potential to compromise the integrity, confidentiality, or availability of information

Terms	Definition
Incident Management	Process of identifying, managing, recording, and analyzing security threats or incidents
Security Training	Programs designed to educate employees about the importance of information security and practices and behaviours that protect the organizations assets.

3.4 ROLES AND RESPONSIBILITIES

Roles	Responsibilities
CTO	Provide approval and official endorsement to this policy
CISO	Reviewing the policy and providing formal support
IT Director	Creation and upkeep of this policy, approving any deviations from its stipulations, and actively encouraging adherence among all stakeholders
Supervisors	Assist employees and contractors in understanding this policy's requirements and promptly address and notify the IT department about any breaches of this policy
Administrators	Ensure that contracts clearly specify the security responsibilities and obligations of all involved parties
Human Resource	Responsible for introducing new employees and contractors to Cybertech's IT and Security policies on their first day of employment and aiding all employees and contractors in understanding this policy's requirements
Users	Expected to report any observed and suspected breaches of this policy to their supervisor, manager, or team lead immediately

4. POLICY STATEMENTS

4.1 Secure Areas

4.1.1 Physical Security Perimeter

4.1.2 Physical Entry Controls

4.1.3 Securing Offices, Rooms, and Facilities

4.1.4 Protecting Against External and Environmental Threats

4.1.5 Working in Secure Areas

4.1.6 Delivery and Loading Areas

4.2 Equipment

4.2.1 Equipment Siting and Protection

4.2.2 Supporting Utilities

4.2.3 Cabling Security

4.2.4 Equipment Maintenance

4.2.5 Removal of Assets

4.2.6 Security of Equipment and Assets Off-Premises

4.2.7 Secure Disposal or Reuse of Equipment

4.2.8 Unattended User Equipment

4.2.9 Clear Desk and Clear Screen Policy

4.1 SECURE AREAS

In order to stop illegal direct entry, harm, and disruption to the company's data and data process infrastructure.

4.1.1 PHYSICAL SECURITY PERIMETER

Data processing plants & locations containing delicate or important data must have protected by designated safety boundaries.

- Physical access control measures will be implemented in a way that is specific to what system needs to be protected, utilizing techniques like:
  - The construction of limits, checks, and surrounding buildings or gates to define secured regions.
  - With simple security requirements, classic key locks that work with physical keys should be used.
  - The implementation of electronic access control systems, which provide a number of choices such as:
    - Crypto locks, that enable programmable access and utilize keypads for entry management.
      - Methods for limiting access via cards, these are further separated into the following categories:
      - With quick access requirements, removable media like magnetic stripe ones can be used.
      - The microchips are incorporated into cards with chips to improve safety and retain information.
      - Managing access is facilitated by biometric technologies, which use distinct individual identification numbers like fingerprints, hand geometry, and recognition of the face.
      - Using each among the previously stated choices to create a multi-factor login solution for better safety.
- In order to strengthen the security of such crucial resources, more security zones are going to be added and enhanced physical security measures will be implemented surrounding locations that house critical data and essential equipment.

- To guarantee relevant and acceptable standards of security, the assignment of access privileges for safe places inside the business shall be reviewed and modified on frequent intervals.

- The primary data center space in the surroundings of the company:
  - It will be protected from additional limited regions by far tougher regulations in order to protect essential facilities & information.
  - Only people who have received express permission from the IT Department will have permitted to enter the area, guaranteeing that just those that truly have are able to be inside.
  - Possible risks can be reduced because entrance rights are restricted those who can prove a valid company requirement.
  - It will only be available to carry out authorized company activities, guaranteeing safety and transparency.
  - To maintain conformity and protection, individuals who are authorized accessibility should thoroughly familiarize themself with as well as abide by the relevant policies governing data center admission.

- Every point of access to a data center has to be kept safely locked at all times, with only necessary operations being permitted to temporarily allow:
  - Enabling authorized people to enter and leave under strict oversight and control, and every move duly recorded.
  - Supervising the safe and controlled transfer of materials or devices, making sure that those having access control are in charge.
  - Remarkably propped up an entrance to increase circulation into the data center in the event of a cooling breakdown, protecting the security of equipment and control systems.

4.1.2 PHYSICAL ENTRY CONTROLS

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

- The Security and Safety Department, in collaboration with the IT Department and Information Security Officer, will develop and implement comprehensive policies and procedures governing physical access to buildings and areas housing the organization's systems (e.g., data center). These policies will reflect the security classification of the systems protected.

- □ The management of visitor entry and exit will be stringent, with security personnel at reception desks or entry gates required to verify visitor identities through widely recognized forms of identification (e.g., Identity Card or Passport). Visitor entry will be contingent upon confirmation from the host employee and verification of the visit's purpose.
- □ Access for contractors' personnel to secure areas or data center facilities will be restricted, granted only as necessary, and subject to close monitoring.
- □ Employee identification protocols will include:
  - Mandatory visible identification for all employees (e.g., ID badges).
  - The issuance of "Visitor" badges for non-employees.
  - ID badges will display names, photographs, and badge numbers only.
  - Access cards will not detail the level of access privileges.
- □ The IT Department, working in conjunction with the Security and Safety Department, will oversee the management and surveillance of CCTV cameras and access control systems within the data center.
- □ All entries to the data center will be meticulously recorded and preserved for a minimum of twelve months, with access logs capturing:
  - Date and time of access attempts.
  - Outcome of the attempt (successful or unsuccessful).
  - Specific access points utilized.
  - Identity of the individual attempting access.
  - Any modifications to access privileges by supervisory personnel.
- □ Visitors and personnel without ongoing data center access needs will be accompanied by an authorized employee at all times and required to sign a visitor control log.
- □ Implementation of a comprehensive access card control system across the facility, featuring:
  - Employee identification and access cards with photos.
  - Detailed logging of each card's usage.
  - Assignment of access rights in alignment with job responsibilities.
  - Procedures to deactivate lost or stolen cards.

4.1.3 Securing Offices, Rooms, and Facilities

Physical security for offices, rooms and facilities shall be designed and applied.

- □ Security measures across all departments, units, and offices will encompass:
  - Perimeter defenses (e.g., smart cards).
  - Facility management protocols.
  - Parking lot security measures.
- □ Facilities storing sensitive information or hosting critical systems will be designed and maintained to safeguard against physical and environmental threats effectively.
- □ Intrusion detection systems will be installed to monitor external doors, accessible windows, and other potential entry points into buildings.
- □ Hazardous or combustible materials will be stored securely, positioned at a safe distance from secure or sensitive areas to mitigate risks.

4.1.4 Protecting Against External and Environmental Threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

- □ The Security and Safety Department will prioritize personnel safety, implementing necessary measures to maintain a secure workplace environment.
- □ Development and documentation of evacuation procedures for emergencies such as fires, floods, earthquakes, or other disasters to safeguard employees and systems.
- □ Environmental controls will be strategically designed and implemented to mitigate damage from various disasters, including fire, flood, earthquakes, explosions, civil unrest, and other natural or man-made incidents.
- □ Emergency equipment, including emergency lighting and fire extinguishers, will be available across facilities, with quarterly inspections to confirm their functionality.
- □ The Datacenter and similar critical areas will be equipped with specific external and environmental controls (e.g., temperature, humidity, dust, atmospheric pressure, electromagnetic radiation, static electricity) in line with manufacturer guidelines.
- □ The IT Department will oversee the physical monitoring of the Datacenter, ensuring central supervision of:

- Physical access controls.
- Ventilation and Air-Conditioning systems.
- Emergency power supplies, including generators and UPS systems.
- Fire detection and suppression systems.
- Water leakage detection systems.
- CCTV surveillance.
- Rack configurations and security.

4.1.5 Working in Secure Areas

Procedures for working in secure areas shall be designed and areas applied.

□ To prevent unwanted access and safeguard assets, the Security and Safety Department will designate secure areas like the Datacenter in coordination with the IT Department and Information Security Officer.

□ Continuous monitoring of sensitive information and critical systems areas through security personnel, CCTV, and intrusion detection systems.

□ Secure storage of all sensitive media (e.g., hard drives, CDs/DVDs), printouts, and manuals in locked containers when not actively in use.

□ Control measures for secure area operations will include:

- Ensuring unattended secure areas remain locked and are regularly checked.
- Restricting the use of recording devices unless explicitly authorized.
- Controlling and supervising third-party support services' access to secure areas.

4.1.6 Delivery and Loading Areas

Access points such as delivery and loading areas and other points areas where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

□ Delivery and loading zones will be regulated and isolated from Cybertech's facilities to prevent unauthorized access or potential damage to sensitive areas, with specific security protocols including:

- Restricted access to the loading area from outside the premises to designated and authorized personnel.
- Design considerations to allow unloading of supplies without delivery staff accessing other areas.

- All incoming parcels to the premises will be received and inspected by reception staff, with a detailed log maintained for tracking and security purposes.

4.2 EQUIPMENT

To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

4.2.1 EQUIPMENT SITING AND PROTECTION

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

□ To safeguard against environmental threats, hazards, and unauthorized access, equipment based on the classification of information and/or systems will be appropriately protected.

□ Security controls for securing all critical systems include:

- Ensuring equipment is housed in a secure location to deter unauthorized access.
- Ensuring that only designated persons can access these locations.
- Monitoring environmental conditions to prevent adverse effects on computer system operations.
- System owners should assess and mitigate potential disasters in nearby areas, such as fires, water damage, or explosions, that could impact system integrity.

□ Criteria for locating Cybertech facilities include, but are not limited to:

- Avoiding public access locations.
- Choosing areas with minimal risk of natural disasters or human-induced damages, like vandalism or fires, including considerations for water damage from internal systems or external sources.

□ All Cybertech equipment, such as servers and network devices, will be securely housed within the data center's protective environment with proper surveillance.

□ Measures will be in place to prevent unauthorized access through bypass booting methods that circumvent password authentication.

□ Security protocols will be established to minimize the risk of sensitive information leakage from equipment in use.

4.2.2 SUPPORTING UTILITIES

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities

- □ The IT Department, in partnership with the Operation and Maintenance Department, will implement power protection strategies to ensure system availability.
- □ Power supply continuity considerations will include:
  - The provision of multiple power feeds to eliminate single points of failure.
  - The recommendation for Uninterruptible Power Supply (UPS) systems to facilitate an orderly shutdown or maintain operation of equipment critical to business functions, with regular testing as per manufacturer guidelines.
  - The inclusion of backup generators for essential processing and business continuity requirements.
- □ Critical systems will be configured for immediate switchover to an alternative power source in the event of power loss.
- □ Protection measures against power failures and electrical anomalies will be enforced, ensuring an electrical supply that meets or exceeds the equipment manufacturer's specifications.
- □ Supporting infrastructure, such as air conditioning and security alarm systems, will receive a reliable electrical supply devoid of surges and interference, potentially utilizing power-conditioning strips to mitigate power surge risks.
- □ UPS systems will undergo routine testing according to manufacturer instructions to guarantee dependable operation.

4.2.3 CABLING SECURITY

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

- □ To safeguard against physical damage and unauthorized access or interception, power, voice, and telecommunication cables will be subject to stringent protection measures, including:
  - Shielding telecommunication cables from wiretapping and ensuring they do not traverse areas accessible to third parties.

- Ensuring data network cabling is securely isolated and routed through protected zones to prevent unauthorized damage or interception.
- Isolating power supply cabling effectively.
- Utilizing armoured conduit and securing inspection and termination points within locked rooms or enclosures.
- Implementing alternative cable routings or transmission media to enhance security.
- Preferring fiber optic cabling for its security and performance advantages.
- Regularly inspecting for and removing unauthorized devices attached to the network.

- Where feasible, cables will be laid underground, avoiding public spaces and utilizing conduit for additional protection against exposure and damage.

4.2.4 EQUIPMENT MAINTENANCE

Equipment shall be correctly maintained to ensure its continued availability and integrity.

□ The IT Department, in collaboration with the Operations and Maintenance Department, will adhere to rigorous maintenance protocols for technical equipment, including servers, network devices, and communication infrastructure, to guarantee their operational integrity and availability. Maintenance controls will encompass:

- Adhering to the manufacturer's recommended service intervals and guidelines.
- Restricting repair and servicing activities to authorized personnel.
- Comprehensive logging of all equipment malfunctions and maintenance actions, both preventive and corrective.

□ Manufacturer-performed maintenance on Cybertech equipment will require formal authorization and oversight to ensure compliance and security.

□ Key considerations for Cybertech equipment management include:

- Securing maintenance contracts for all critical Cybertech equipment to guarantee service availability and business continuity.
- Ensuring maintenance contracts encompass both routine and emergency servicing needs.
- Validating that maintenance agreements provide for regular servicing, support, and spare parts.
- Supervising maintenance operations by designated personnel.

- Receiving monthly maintenance reports from vendors to monitor equipment health and status consistently.
- Maintaining a detailed schedule and log for data center maintenance activities by the IT Department to ensure timely servicing and to track any pertinent issues effectively.

4.2.5 Removal Of Assets

Equipment, information or software shall not be taken off-site without prior authorization.

□ Removal of Cybertech equipment, assets, or software from the premises without appropriate authorization is prohibited. When necessary, the following protocols must be observed:

- Personnel must secure proper authorization to take equipment off-site.
- Equipment must be logged out before removal.
- Time limits for off-site use should be established.
- Upon return, equipment must be logged back in.

4.2.6 Security of Equipment and Assets Off-Premises

Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

□ The IT Department will enforce stringent controls for sending Cybertech equipment off the premises for maintenance, which include:

- Ensuring equipment is properly packaged and sealed.
- Storing equipment in safe and secure locations.
- Providing clear and complete shipping and tracking instructions.

□ Authorization from the asset's owner is required before equipment is moved off the premises for maintenance or repair, with all movements duly recorded.

□ All portable Cybertech equipment (e.g., laptops, mobile phones) must be:

- Stored securely in locked cabinets, credenzas, or with vinyl-covered steel cables when not in use.
- Physically secured with an appropriate security device when unattended.

- □ Portable Cybertech equipment should avoid storing sensitive information locally, favoring network file servers. Any removable media must be securely stored according to its sensitivity.

4.2.7 Secure Disposal or Reuse of Equipment

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

- □ The IT Department will develop procedures for:
  - The disposal of confidential documents.
  - The destruction of computer equipment containing sensitive information.
  - The sanitization of equipment prior to sale or transfer.
  - The destruction of various types of media.
- □ Sensitive information on storage media no longer needed must be securely erased or physically destroyed, including:
  - Rewritable media being securely erased through multiple overwrites.
  - Paper documents being shredded.
- □ Disposal records, including disposal requests and approvals, will be maintained.
- □ Prior to disposal or reuse, Cybertech equipment and media will be inspected to ensure sensitive information and licensed software have been removed or overwritten.
- □ The destruction of sensitive information on storage media will proceed only with approved methods.

4.2.8 Unattended User Equipment

Users shall ensure that unattended equipment has appropriate protection.

- □ The IT Department will activate password-protected screen savers on all servers and workstations, set to engage after no more than 10 minutes of inactivity.
- □ Users are responsible for terminating sessions upon completion of activities and locking their equipment when leaving their desks.

4.2.9 Clear Desk and Clear Screen Policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

- To enforce a clear desk and screen policy, users must adhere to guidelines including:
  - Secure storage of paper and media in locked cabinets or secure furniture when not in use.
  - Sensitive documentation should be locked away, ideally in fire-resistant storage, particularly when offices are unoccupied.
  - Workstations and printers should not remain logged in when unattended, protected by password-protected screen savers
  - Photocopiers and fax machines should be secured with PIN codes outside of working hours
  - Confidential printed information must be promptly removed from printers
- Department Managers are tasked with communicating and monitoring adherence to the clear desk and screen policy within their teams
- The Information Security Officer, in collaboration with the Personnel Affairs Department, will ensure all employees receive appropriate awareness training on the clear desk and screen policy

5. POLICY COMPLIANCE

5.1 COMPLIANCE MEASUREMENT

- Cybertech's information security management team will ensure staff and guests will follow this policy by having reports from business tools, internal and external audits, and through feedback to the owner of this policy

5.2 EXCEPTIONS

- Any exception to the policy need to be approved and documented beforehand by Cybertech's information security management team. Exceptions will be reviewed by the management review team

5.3 NON-COMPLIANCE

- If an employee is found violating this policy, corrective action will be taken against them, which can be escalated to the point of job termination

5.4 CONTINUAL IMPROVEMENT

- As part of its continuous improvement process, this policy will be reviewed and revised at regular intervals