CYBERSECURITY POLICY

justdareus

CYBERCOHORTS Calgary, Alberta

Table of Contents

Introduction

At CyberCohorts, a trusted provider of cybersecurity and data analysis training, protecting the Confidentiality, Integrity, and Availability (CIA) of our digital assets is critical to our operations and the trust we maintain with our clients and stakeholders. This cybersecurity policy establishes a clear and actionable framework to safeguard our systems, networks, and data from cyber threats, ensuring secure and reliable operations that align with our business goals.

The principles of Confidentiality, Integrity, and Availability—foundations of effective cybersecurity—are defined as follows:

Confidentiality: Ensuring sensitive information is accessible only to authorized individuals or systems, enforced through robust access controls and the "need-to-know" principle.

Integrity: Maintaining the accuracy and reliability of data by preventing and detecting unauthorized modifications or corruption.

Availability: Ensuring that critical systems, networks, and information remain accessible and operational for authorized users when needed.

This policy provides the foundation for CyberCohorts' cybersecurity strategy, supporting the implementation of effective controls, processes, and standards. It is designed to protect our digital ecosystem and the data entrusted to us by our clients, partners, and other stakeholders, enabling us to meet the demands of a secure and evolving digital landscape.

Purpose

The purpose of the CyberCohorts Cybersecurity Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to CyberCohorts, its business partners, its clients and its stakeholders.

Scope

The CyberCohorts Cybersecurity Policy applies equally to all individuals and entities with access to CyberCohort's information systems, applications, and data. This includes employees, contractors, and third-party vendors, regardless of their role or level of access.

The policy covers all digital assets owned, managed, or operated by CyberCohorts, including on-premises infrastructure, cloud-based systems, and any devices or platforms used to access organizational data. It establishes expectations for the secure handling of CyberCohorts'

information assets to ensure the protection of sensitive data and the integrity of the organization's operations.

Responsibilities

The effectiveness of CyberCohorts's cybersecurity efforts relies on clear roles and active participation from all individuals within the organization. Key responsibilities are outlined below:

Executive Management

- Ensure that an appropriate risk-based Cybersecurity Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of CyberCohorts.
- Provide sufficient financial and personnel resources to implement and maintain cybersecurity practices.
- Appoint a Cybersecurity Lead and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Cybersecurity Lead reports annually to Executive Management on the effectiveness of the CyberCohorts Cybersecurity Program.

Cybersecurity Lead

- Oversee the development, implementation, and management of CyberCohorts's cybersecurity program.
- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Develop and implement a process to identify and address cybersecurity risks, including those related to third-party vendors.
- Ensure compliance with laws, regulations, and standards.
- Conduct training and awareness programs to educate employees and stakeholders on cybersecurity responsibilities.
- Monitor and evaluate the effectiveness of cybersecurity controls and report findings to Executive Management.
- As the organization expands, chair the Cybersecurity Committee, a critical governance body within Cybercohorts that will be responsible for overseeing and guiding the implementation, management, and continuous improvement of cybersecurity practices.

All Employees, Contractors, and Other Third-Party Personnel

All individuals with access to CyberCohorts's systems and data are critical to maintaining the organization's cybersecurity posture. Their responsibilities include:

- Compliance: Formally sign off and agree to abide by the policies, standards, and guidelines outlined in this cybersecurity policy and any supporting procedures.
- Secure Use of Resources: Use CyberCohorts's information systems and data responsibly, ensuring that access is limited to authorized purposes and sensitive information is handled appropriately.
- Training and Awareness: Complete all required cybersecurity training and actively participate in awareness programs to stay informed about potential threats, secure practices, and CyberCohorts's security requirements.
- Incident Reporting: Promptly report any observed or suspected security incidents, unauthorized access, vulnerabilities, or policy violations to the Cybersecurity Lead or designated contact.
- Accountability: Take personal responsibility for protecting CyberCohorts's systems and data by adhering to access controls, password policies, and secure practices when interacting with organizational resources.

Statement of Policy

This Statement of Policy outlines the measures necessary to protect CyberCohorts' assets, comply with legal and regulatory obligations, and support its mission as a trusted training provider.

1. Confidential Data

CyberCohorts recognizes the importance of protecting confidential data, defined as information whose unauthorized access, disclosure, modification, or loss could result in significant damage to the company, partners, affiliates, or customers. Examples of confidential data include, but are not limited to:

- Unpublished financial information.
- Credit card numbers.
- Customer,student, partner, and vendor data.
- Human resources records.
- Proprietary information such as patents, formulas, and new technologies.

Protection of confidential data is the responsibility of all employees, contractors, and third parties with access to Cybercohorts' systems. Everyone must actively follow these practices to prevent unauthorized access or disclosure.

2. Compliance with Regulatory and Legal Requirements

CyberCohorts complies with all relevant cybersecurity standards, laws, and contractual obligations, including but not limited to:

- GDPR (General Data Protection Regulation) for data protection and privacy.
- PCI DSS (Payment Card Industry Data Security Standard) for securely processing credit card payments.
- State and federal breach notification laws for timely incident reporting.
- NIST Cybersecurity Framework (CSF) and ISO 27001 for cybersecurity best practices.
- Any other contractual requirements with clients, partners, or vendors.

3. User Access and Access Control

CyberCohorts enforces strict access control measures to minimize risks of unauthorized access to its systems and data:

- **Role-Based Access:** Access is granted based on role and need-to-know principles.
- **Access Approvals:** All access requests must be formally approved and documented.
- **Periodic Reviews:** Access rights are reviewed regularly to ensure they remain valid and necessary.
- **Deactivation:** User accounts are promptly deactivated when no longer required (e.g., employee termination).
- **Shared Accounts:** Shared accounts are discouraged and require explicit management approval.

4. Data Security

- **Multi-Factor Authentication (MFA):** All internet-facing systems and sensitive applications must require MFA for access.
- **Password Management Policies:** Employees must create strong, unique passwords with a minimum of 12 characters, including upper/lowercase letters, numbers, and symbols. Passwords must be changed every 30 days or immediately upon suspicion of compromise.
- **Device Security:** All devices (including mobile phones and tablets) must have secure authentication mechanisms enabled.

5. Data Protection and Privacy

CyberCohorts protects sensitive and confidential data through a combination of encryption, access controls, and secure handling practices:

- **Data Classification**: Data is classified to determine appropriate security measures, with extra protection for customer, partner, and employee information.
- **Data Encryption**: Sensitive data must be encrypted at rest and in transit using industry standards.
- **Data Transfers**: Sensitive data transfers are prohibited unless encrypted and conducted via CyberCohorts-approved channels.
- **Storage**: Confidential data must only be stored on authorized systems or drives with restricted access.
- **Retention and Disposal**: Data is retained only as long as necessary and securely destroyed when no longer needed.

6. Network and Systems Security

CyberCohorts ensures the integrity and availability of its networks and systems through:

- Firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and block unauthorized traffic.
- Secure configuration of systems and devices to minimize vulnerabilities.
- Regular patch management to ensure systems are up to date and protected against known threats.
- Network segmentation to limit access to sensitive data.

7. Incident Response

CyberCohorts is prepared to respond promptly to cybersecurity incidents:

- **Reporting**: All employees, contractors, and third parties must report suspicious activities, phishing attempts, or breaches immediately to the Cybersecurity Lead.
- **Response Process**: The incident response plan includes detection, containment, eradication, recovery, and post-incident analysis.
- **Companywide Alerts**: When necessary, CyberCohorts will issue alerts to notify employees of active threats or required precautions.

8. Security Awareness and Training

Cybersecurity awareness is a core priority at CyberCohorts:

- **Employee Training**: All employees and contractors must complete mandatory cybersecurity training, including secure password practices, phishing awareness, and proper data handling.
- **Ongoing Awareness**: CyberCohorts regularly updates employees on new threats, such as scam emails, malware, and social engineering tactics.

9. Remote Work Security

Employees working remotely must adhere to all aspects of this policy:

- Use only company-approved devices and secure networks for accessing CyberCohorts systems.
- Avoid public Wi-Fi; use a VPN when necessary.
- Report any concerns about home network security to the IT team for evaluation.

10. Additional Security Measures

To further mitigate risks, CyberCohorts requires:

- Devices and screens to be locked when unattended.
- Suspicious websites, emails, or unauthorized software to be avoided and reported.
- Immediate reporting of lost, stolen, or compromised devices to the IT team.
- Compliance with CyberCohorts's social media and data handling policies to prevent accidental data leaks.

11. Enforcement and Disciplinary Actions

Cybercohorts considers cybersecurity a shared responsibility. Employees who fail to comply with this policy will face disciplinary actions based on the severity of the breach:

- **First-time, unintentional violations**: A verbal warning, additional training, or suspension of access may apply.
- **Intentional or repeated violations**: Severe actions, including termination or legal consequences, may result.

All incidents will be reviewed on a case-by-case basis, considering the impact on CyberCohorts, its customers, and its partners.

12. Commitment to Cybersecurity

At CyberCohorts, we recognize that the trust of our students, partners, and employees depends on a proactive approach to cybersecurity. Every individual within the organization contributes to this mission by following the best practices and being vigilant against potential threats.

By adhering to this policy, we ensure the security and privacy of our systems, allowing us to fulfill our mission as a trusted cybersecurity training provider.

Waivers

In certain situations, exceptions to this Cybersecurity Policy may be required to address unique business needs or operational circumstances. Waivers to the policy will only be granted under the following conditions:

1. Formal Request: A written request must be submitted to the Cybersecurity Lead, detailing the specific policy provision for which a waiver is being sought, the justification, and the proposed duration of the waiver.
2. Approval Process: Waivers must be reviewed and approved by Executive Management in consultation with the Cybersecurity Lead.
3. Documentation: Approved waivers must be documented, including the scope, rationale, duration, and any associated risks or mitigation measures.
4. Periodic Review: Waivers will be reviewed periodically to ensure they remain valid and necessary, with corrective actions implemented if required.

Unapproved deviations from this policy may result in disciplinary action.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Policy Review and Updates

The policy will be reviewed annually or in response to significant changes in the business environment or regulatory requirements. The review and updates shall be carefully deliberated with the Executive Management, Cybersecurity Lead, IT personnel and the Cybersecurity

Committee (when established) to keep up with the changes in the regulatory environment, business operations, or threat landscape.

All updates will be communicated to employees, contractors, and other relevant parties. Updated versions will be distributed, and employees will be required to acknowledge their understanding and compliance.

Management Commitment

This policy is supported and approved by:

Name/ CEO .....

Date .....

Name/ Cybersecurity Lead .....

Date .....

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	December 2024			Document Origination