## 

## Acceptable Use Policy

## 

**Document Number**: ISMS-PL-02  
 **Version**: 1.0  
 **Last Updated**: July 18, 2025  
 **Document Owner**: Head of Information Security  
 **Internal Use Only**

### Document Control

**Document Approvals**

This document has been reviewed and approved by:

|  |  |  |
| --- | --- | --- |
| Prepared By | Reviewed By | Approved By |
| IT Security Team | Head of Information Security | Chief Technology Officer |
| July 18, 2025 | July 18, 2025 | July 18, 2025 |

### Version History

The following table lists all the revisions made to this document:

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Revised By** |
| 1.0 | July 18, 2025 | Initial Draft & Release | ISMS Governance Team |

### Reference Standards

|  |  |  |
| --- | --- | --- |
| **Standard** | **Clause Reference** | **Requirement** |
| ISO/IEC 27001:2022 | A.5–A.18 | ISMS Controls & Acceptable Use |
| ISO/IEC 27701:2019 | CL.6.5.1–CL.6.15.2 | Privacy Information Management |
| HIPAA / GDPR / PIPEDA | Regulatory Compliance | Healthcare Data & Personal Information |
| CyberDyne ISMS Framework | Policy Ref ISMS-PL-01 | Internal Information Security Controls |

Contents

[Acceptable Use Policy 1](#_Toc203770862)

[Document Control 2](#_Toc203770863)

[Version History 2](#_Toc203770864)

[Reference Standards 2](#_Toc203770865)

[1. Purpose 3](#_Toc203770866)

[2. Scope 4](#_Toc203770867)

[3. Definition 4](#_Toc203770868)

[4. Acceptable Use Policy 4](#_Toc203770869)

[I. Protection of Cyberdyne Information and Systems 4](#_Toc203770870)

[II. Sensitive Information and Handling 4](#_Toc203770871)

[III. Use of CyberDyne Systems and Equipment 4](#_Toc203770872)

[IV. Email & Messaging Guidelines 4](#_Toc203770873)

[V. Internet Access & Remote Connectivity 4](#_Toc203770874)

[VI. Mobile Devices & Removable Media Controls 4](#_Toc203770875)

[VII. User Accounts, Passwords & Authentication 4](#_Toc203770876)

[VIII. Physical & Network Security 5](#_Toc203770877)

[IX. Telephone, Fax, and Printer Use 5](#_Toc203770878)

[X. Employee Obligations and Legal Compliance 5](#_Toc203770879)

[XI. Prohibited Activities 5](#_Toc203770880)

[5. Incident Reporting Procedures 5](#_Toc203770881)

[6. Monitoring and Enforcement 5](#_Toc203770882)

[7. Supporting Policies 5](#_Toc203770883)

## Purpose

The purpose of this Acceptable Use Policy is to define the guidelines for responsible, secure, and lawful usage of CyberDyne Health’s information systems and resources. This policy ensures that employees and third parties understand their obligations to protect sensitive healthcare data, uphold the organization’s security standards, and minimize operational and reputational risks arising from misuse.

It supports compliance with internal information security policies and external regulations (e.g., HIPAA, GDPR, PIPEDA), and reinforces CyberDyne Health’s commitment to safeguarding patient trust, business integrity, and technological resilience.

## Scope

This policy applies to all individuals accessing CyberDyne Health systems, networks, and data— including employees (permanent and temporary), contractors, partners, business associates, vendors, and authorized third parties.

## Definition

Sensitive Information: Any data labelled *Confidential* or *Highly Confidential* under the CyberDyne Information Classification Policy, especially Protected Health Information (PHI), Personally Identifiable Information (PII), and regulated clinical research data.

Assets: Includes hardware (laptops, servers), software, network infrastructure, storage media, and any tools owned or operated by Cyberdyne Health.

## Acceptable Use Policy

### Protection of Cyberdyne Information and Systems

Users must preserve confidentiality, integrity, and availability of assets; system usage may be monitored without prior notice.

### Sensitive Information and Handling

Data must be classified appropriately. Sensitive data requires encryption, authorized disclosure, and proper physical/electronic protection. Breaches must be reported immediately.

### Use of CyberDyne Systems and Equipment

Only approved devices/software may be used for official work. Screen locks, secure workspaces, and clear desk/screen practices are mandatory.

### Email & Messaging Guidelines

Email must be professional, secure, and encrypted when necessary. Spam, impersonation, or sharing confidential info without approval is prohibited.

### Internet Access & Remote Connectivity

Browsing must be through secure gateways. VPN and MFA are required for remote access. Access to illegal content or bypassing filters is prohibited.

### Mobile Devices & Removable Media Controls

Removable devices require IT clearance and encryption. Data must be handled and stored securely. Unauthorized use or transfer is prohibited.

### User Accounts, Passwords & Authentication

Credentials must be unique, strong, confidential, and rotated. Shared accounts are prohibited. MFA must be implemented for critical systems.

### Physical & Network Security

Offices must remain secure. Visitors require badges. Equipment must be locked or removed only by authorized individuals.

### Telephone, Fax, and Printer Use

Sensitive info must not be left in shared areas or transmitted over unsecured lines. Identity must be verified before verbal disclosure.

### Employee Obligations and Legal Compliance

Users must follow policy, avoid infringing laws, and refrain from misusing organizational resources. Systems may be monitored to ensure compliance.

### Prohibited Activities

Includes unauthorized software use, credential sharing, data manipulation, network sniffing, and inappropriate social media posts relating to CyberDyne or its stakeholders.

## Incident Reporting Procedures

All violations, security events, or suspicious activities must be promptly reported to supervisors or the Information Security Team by emailing security@vyber.com

## Monitoring and Enforcement

CyberDyne reserves the right to monitor systems. Violations may result in disciplinary action, legal proceedings, or termination of access.

## Supporting Policies

1. Data Management Policy
2. Information Security Policy Framework
3. Network Management Policy
4. Cryptography Policy
5. Mobile Device and Teleworking Policy
6. Access Control Policy
7. Third Party Management Policy
8. Security Incident Management Procedure
9. Physical Security Policy
10. Business Continuity and Disaster Recovery Plan
11. Code of Conduct and HR Security Policy

End of Document