| Basic Cyber Hygiene Policy | | | | | |
|---|---|---|---|---|---|
| Policy # | IS.02.00 | Revision # | 3.0 | Effective Date | 2021-10-01 |

# Table of Contents



# Purpose

This policy establishes the core security defenses necessary to defend against the most common security threats. This policy must be implemented regardless of risk.

Refer to the Information Security Charter for additional guidance.

# Scope

This policy applies to all employees, partners, and third parties with access to WEC Group Ltd information assets.

# Policies and Controls

The policy and control numbering scheme map directly to version 8 of the CIS Controls. (https://www.cisecurity.org/controls/cis-controls-navigator/)

## 1 Inventory and Control of Enterprise Assets

WEC Group Ltd must actively manage all enterprise IT assets and remediate unauthorized and unmanaged assets connected to the network.

**Controls:**

- 1.1 Establish and Maintain Detailed Enterprise Asset Inventory
- 1.2 Address Unauthorized Assets

## 2 Inventory and Control of Software Assets

WEC Group Ltd must actively manage all software assets and configure systems to only permit the installation and execution of authorized software.

**Controls:**

- 2.1 Establish and Maintain a Software Inventory
- 2.2 Ensure Authorized Software is Currently Supported
- 2.3 Address Unauthorized Software

## 3 Data Protection

WEC Group Ltd must develop procedures and technical safeguards to identify, classify, securely handle, retain, and dispose of data, regardless of location; including, but not limited to: Company Owned Infrastructure, Cloud Services, and Mobile Devices.

**Controls:**

- 3.1 Establish and Maintain a Data Management Process
- 3.2 Establish and Maintain a Data Inventory
- 3.3 Configure Data Access Control Lists
- 3.4 Enforce Data Retention
- 3.5 Securely Dispose of Data

- 3.6 Encrypt Data on End-User Devices

## 4 Secure Configuration of Enterprise Assets and Software

The IT Department must establish and maintain secure configuration baselines and/or standards for enterprise IT assets and software. The IT Department will develop procedures to ensure the baseline security configuration is applied consistently to all devices and operating systems.

**Controls:**

- 4.1 Establish and Maintain a Secure Configuration Process
- 4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure
- 4.3 Configure Automatic Session Locking on Enterprise Assets
- 4.4 Implement and Manage a Firewall on Servers
- 4.5 Implement and Manage a Firewall on End-User Devices
- 4.6 Securely Manage Enterprise Assets and Software
- 4.7 Manage Default Accounts on Enterprise Assets and Software

## 5 Account Management

The IT Department must develop procedures and implement technical safeguards to assign and manage authorization of user accounts, including privileged accounts and service accounts, for all enterprise IT assets and software.

**Controls:**

- 5.1 Establish and Maintain an Inventory of Accounts
- 5.2 Use Unique Passwords
- 5.3 Disable Dormant Accounts
- 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts

## 6 Access Control Management

WEC Group Ltd's management team, in coordination with its IT Department, must establish procedures to manage access control across all enterprise IT assets and software. The procedures must include user on and off boarding processes, privilege management, and strong authentication mechanisms (e.g. MFA, strong password policies).

**Controls:**

- 6.1 Establish an Access Granting Process
- 6.2 Establish an Access Revoking Process
- 6.3 Require Multi-Factor Authentication (MFA) for Externally-Exposed Applications
- 6.4 Require Multi-Factor Authentication (MFA) for Remote Network Access
- 6.5 Require Multi-Factor Authentication (MFA) for Administrative Access

## 7 Continuous Vulnerability Management

The IT Department must establish a vulnerability management program that continuously scans and tracks vulnerabilities on all enterprise IT assets and software. In addition to tracking vulnerabilities, the program must establish procedures and processes to deploy patches and remediate vulnerabilities based on CVSS scores and the inherent risk the vulnerability presents to the enterprise.

**Controls:**

- 7.1 Establish and Maintain a Vulnerability Management Process
- 7.2 Establish and Maintain a Remediation Process
- 7.3 Perform Automated Operating System Patch Management
- 7.4 Perform Automated Application Patch Management

## 8 Audit Log Management

The IT Department must implement log management procedures and technology that facilitates the collection, analysis, alerting, and retention of audit logs across all enterprise IT assets and software.

**Controls:**

- 8.1 Establish and Maintain an Audit Log Management Process
- 8.2 Collect Audit Logs
- 8.3 Ensure Adequate Audit Log Storage

## 9 Email and Web Browser Protections

The IT Department must implement technical safeguards to protect against email and web browsing based attacks.

**Controls:**

- 9.1 Ensure Use of Only Fully Supported Browsers and Email Clients
- 9.2 Use DNS Filtering Services

## 10 Malware Defenses

The IT Department must implement malware defenses to prevent the installation, spread, and execution of malicious applications, code, or scripts on enterprise IT assets.

**Controls:**

- 10.1 Deploy and Maintain Anti-Malware Software
- 10.2 Configure Automatic Anti-Malware Signature Updates
- 10.3 Disable Autorun and Autoplay for Removable Media

## 11 Data Recovery

WEC Group Ltd's management team, in coordination with its IT Department, must establish and maintain a disaster recovery plan capable of restoring systems to a pre-incident and trusted state. The recovery capability must prioritize the data recovery capabilities according to the criticality of the IT system and its related data.

**Controls:**

- 11.1 Establish and Maintain a Data Recovery Process
- 11.2 Perform Automated Backups
- 11.3 Protect Recovery Data
- 11.4 Establish and Maintain an Isolated Instance of Recovery Data

## 12 Network Infrastructure Management

The IT Department must implement procedures and technology to actively manage WEC Group Ltd's IT Infrastructure. This includes but is not limited to, maintaining serviceable hardware, modern operating systems, network documentation, utilizing secure management protocols, segmenting network services into security zones, and where possible, leveraging centralized authentication, authorization, and auditing.

**Controls:**

- 12.1 Ensure Network Infrastructure is Up-to-Date

## 13 Network Monitoring and Defense

The IT Department must establish procedures and implement technical safeguards to maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

**Controls:**

- See IS.03.00 Enhanced Cyber Hygiene Policy

## 14 Security Awareness and Skills Training

WEC Group Ltd's management team, in coordination with its IT Department, must establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

**Controls:**

- 14.1 Establish and Maintain a Security Awareness Program
- 14.2 Train Workforce Members to Recognize Social Engineering Attacks
- 14.3 Train Workforce Members on Authentication Best Practices
- 14.4 Train Workforce on Data Handling Best Practices

- 14.5 Train Workforce Members on Causes of Unintentional Data Exposure
- 14.6 Train Workforce Members on Recognizing and Reporting Security Incidents
- 14.7 Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
- 14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

### 15 Service Provider Management

WEC Group Ltd's management team, in coordination with its IT Department, must develop a procedure to evaluate service providers who hold sensitive data, or are responsible for an enterprise’s critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

**Controls:**

- 15.1 Establish and Maintain an Inventory of Service Providers

### 16 Application Software Security

- See IS.03.00 Enhanced Cyber Hygiene Policy

### 17 Incident Response Management

WEC Group Ltd's management team, in coordination with its IT Department, must establish and maintain an incident response plan to prepare, detect, and quickly respond to an attack.

**Controls:**

- 17.1 Designate Personnel to Manage Incident Handling
- 17.2 Establish and Maintain Contact Information for Reporting Security Incidents
- 17.3 Establish and Maintain an Enterprise Process for Reporting Incidents

### 18 Penetration Testing

- See IS.03.00 Enhanced Cyber Hygiene Policy

## References

1. https://www.cisecurity.org/controls
2. https://www.cisa.gov/cyber-essentials
3. https://www.nist.gov/cyberframework

# Revision History

| Version | Description | Revision Date | Review Date | Reviewer |
|---|---|---|---|---|
| 3.0 | Align IT Security Policies with v8 of CIS Controls and simplify text | 2021-08-18 | 2021-10-01 | Kraig Schario |

# Approval and Ownership

| Approved By | Title | Date | Signature |
|---|---|---|---|
| Kraig Schario | VP Information Technology | 2021-10-01 | On File |