Enhanced Cyber Hygiene Policy					
Policy #	IS.03.00	Revision #	3.0	Effective Date	2021-10-01

Table of Contents

Purpose

This policy builds upon the "Basic Cyber Hygiene Policy". This policy and its controls address increased levels of risk and operational complexity and incorporates safeguards to address existing security threats.

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/)

2 Inventory and Control of Software Assets

□ 2.4 Utilize Automated Software Inventory Tools

3 Data Protection

□ 3.10 Encrypt Data in Transit
□ 3.11 Encrypt Data at Rest

4 Secure Configuration of Enterprise Assets and Software

□ 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
□ 4.9 Configure Trusted DNS Servers on Enterprise Assets
□ 4.10 Enforce Automatic Device Lockout on Portable End-User Devices
□ 4.11 Enforce Remote Wipe Capability on Portable End-User Devices

5 Account Management

□ 5.5 Establish and Maintain an Inventory of Service Accounts

6 Access Control Management

□ 6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems

7 Continuous Vulnerability Management

□ 7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets
□ 7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
□ 7.7 Remediate Detected Vulnerabilities

8 Audit Log Management

- □ 8.4 Standardize Time Synchronization
- □ 8.5 Collect Detailed Audit Logs
- □ 8.9 Centralize Audit Logs
- □ 8.10 Retain Audit Logs
- □ 8.11 Conduct Audit Log Reviews

9 Email and Web Browser Protections

- □ 9.3 Maintain and Enforce Network-Based URL Filters
- □ 9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
- □ 9.5 Implement DMARC
- □ 9.6 Block Unnecessary File Types
- □ 9.7 Deploy and Maintain Email Server Anti-Malware Protections

10 Malware Defenses

- □ 10.4 Configure Automatic Anti-Malware Scanning of Removable Media
- □ 10.6 Centrally Manage Anti-Malware Software

11 Data Recovery

- □ 11.5 Test Data Recovery

12 Network Infrastructure Management

- □ 12.2 Establish and Maintain a Secure Network Architecture
- □ 12.3 Securely Manage Network Infrastructure
- □ 12.4 Establish and Maintain Architecture Diagram(s)
- □ 12.5 Centralize Network Authentication, Authorization, and Auditing (AAA)
- □ 12.6 Use of Secure Network Management and Communication Protocols
- □ 12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise’s AAA Infrastructure

13 Network Monitoring and Defense

- □ 13.1 Centralize Security Event Alerting
- □ 13.3 Deploy a Network Intrusion Detection Solution
- □ 13.4 Perform Traffic Filtering Between Network Segments
- □ 13.5 Manage Access Control for Remote Assets
- □ 13.6 Collect Network Traffic Flow Logs

15 Service Provider Management

- □ 15.2 Establish and Maintain a Service Provider Management Policy
- □ 15.3 Classify Service Providers

16 Application Software Security

Where applicable, the IT Department must establish procedures and technical safeguards to manage the security life cycle of in-house developed, hosted, or acquired software.

□ 16.1 Establish and Maintain a Secure Application Development Process
□ 16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities
□ 16.5 Use Up-to-Date and Trusted Third-Party Software Components
□ 16.7 Use Standard Hardening Configuration Templates for Application Infrastructure
□ 16.8 Separate Production and Non-Production Systems
□ 16.9 Train Developers in Application Security Concepts and Secure Coding
□ 16.10 Apply Secure Design Principles in Application Architectures

17 Incident Response Management

□ 17.4 Establish and Maintain an Incident Response Process
□ 17.5 Assign Key Roles and Responsibilities
□ 17.6 Define Mechanisms for Communicating During Incident Response
□ 17.7 Conduct Routine Incident Response Exercises
□ 17.8 Conduct Post-Incident Reviews

18 Penetration Testing

The IT Department must establish a security testing program that simulates the objectives and actions of an attacker. This program is necessary to test the effectiveness and resiliency of enterprise assets by identifying and exploiting weaknesses in people, processes, and technology. The program must incorporate a remediation process to address any issues discovered during the testing process.

□ 18.1 Establish and Maintain a Penetration Testing Program
□ 18.2 Perform Periodic External Penetration Tests
□ 18.3 Remediate Penetration Test Findings

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