Cybersecurity Guidelines					
Policy #	IS.05.00	Revision #	3.0	Effective Date	2021-10-01

Table of Contents

Purpose

This guideline presents a set of recommended security controls and safeguards. WEC Group Ltd's IT Department should select from these controls based on its risk profile and available resources.

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.

Guidelines

The guideline 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

- 2.5 Allowlist Authorized Software

3 Data Protection

- 3.7 Establish and Maintain a Data Classification Scheme
- 3.8 Document Data Flows
- 3.9 Encrypt Data on Removable Media
- 3.12 Segment Data Processing and Storage Based on Sensitivity

5 Account Management

- 5.6 Centralize Account Management

6 Access Control Management

- 6.7 Centralize Access Control

8 Audit Log Management

- 8.6 Collect DNS Query Audit Logs
- 8.7 Collect URL Request Audit Logs
- 8.12 Collect Service Provider Logs

10 Malware Defenses

- 10.5 Enable Anti-Exploitation Features

12 Network Infrastructure Management

- 12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work

13 Network Monitoring and Defense

- 13.2 Deploy a Host-Based Intrusion Detection Solution
- 13.7 Deploy a Host-Based Intrusion Prevention Solution

15 Service Provider Management

- 15.4 Ensure Service Provider Contracts Include Security Requirements

- 15.6 Monitor Service Providers

16 Application Software Security

- 16.3 Perform Root Cause Analysis on Security Vulnerabilities
- 16.4 Establish and Manage an Inventory of Third-Party Software Components
- 16.11 Leverage Vetted Modules or Services for Application Security Components
- 16.12 Implement Code-Level Security Checks
- 16.13 Conduct Application Penetration Testing

17 Incident Response Management

- 17.9 Establish and Maintain Security Incident Thresholds

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