Information Security Charter					
Policy #	IS.01.00	Revision #	3.0	Effective Date	2021-10-01

Table of Contents

Charter

Objective

WEC Group Ltd recognizes that information and IT assets are critical business assets. It is the responsibility of all users to ensure the safeguarding of business assets. WEC Group Ltd implements, maintains and monitors a comprehensive enterprise information security policy and compliance program appropriate to:

- The risks of the business
- Generally accepted information security practices
- Applicable legal and regulatory requirements

Motivation

WEC Group Ltd values the ability to openly communicate and share information. WEC Group Ltd information (whether belonging to WEC Group Ltd or held in trust on behalf of its clients and business partners) is an important asset that shall be protected according to its value and the degree of damage that could result from its misuse, unavailability, destruction, unauthorized disclosure or modification. Improper disclosure or destruction of these assets may result in harm to the business. Information assets are identified, valued, assessed for risk and protected as appropriate to the needs and risks of the business. Users are required to abide by this WEC Group Ltd's Enterprise Information Security Charter and subsequent policies and procedures.

Principle Goals

Information security is a risk management discipline addressing the preservation of information **confidentiality**, **integrity** and **availability**. The information security effort is established via a hierarchical set of policies and procedures that help users and administrators to define and mitigate risks, maintaining a trade-off between information value and cost of risk mitigation. Policies are high-level documents used to put information security principles into practice. Procedures are a series of related activities aimed at achieving a set of objectives in a measurable and repeatable manner.

- **Principle 1** — Information security policies, standards, guidelines, and procedures are developed to communicate security requirements and guide the selection and implementation of security control measures.

- **Principle 2** — Personal accountability and responsibility for information security are incorporated in roles and responsibilities that ensure that every individual applies the applicable information security policies, principles, procedures and practices in their daily work-related activities.

- **Principle 3** — Information security education, training and awareness programs ensure that users are aware of security threats and concerns and are equipped to apply organizational security policies and principles.

- **Principle 4** — Information assets are classified according to their criticality to the organization enabling an appropriate level of protection. The WEC Group Ltd Information Classification Policy is used to classify information assets.
- **Principle 5** — Information assets are to be used for the intended business purpose only.
- **Principle 6** — Legal, regulatory and contractual requirements are identified, documented and followed.
- **Scope** — It is intended that information is protected in whatever form, including, but not limited to, paper documents, electronic data and the spoken word. Information should be protected while at rest and when it is handled, transmitted or conveyed. IT assets include all devices and hardware/software components of the IT infrastructure, applications and data stores.
- **Action** — All employees and contractors have a responsibility to report suspected security failures or policy violations.

Roles and Responsibilities

- **Executive Management** — Executive managers are accountable for information security and must ensure compliance with security policies, standards, procedures and practices within their respective areas of responsibility.

  Executive management:
  - Will incorporate cybersecurity requirements into its business planning processes.
  - Will allocate the resources (people, processes, and technology) required to protect its information systems as part of its capital planning and investment control processes.

- **Information Security Leadership** — The *Information Security Leader* is responsible for ensuring that appropriate security controls are in existence and in force throughout the enterprise. The leader is responsible for determining methods of implementing and enforcing security policies and for advising the enterprise on security-related issues. The leader ensures, in particular, that information security awareness is increased, and audits are performed and reported regularly. The leader appoints and manages suitably skilled people to staff information security teams as deemed appropriate, and the leader has the authority to request the appointment of security representatives in business units.
- **Security Policy and Compliance Governance** — Security policy and compliance governance is provided by a multidisciplinary group that reviews and endorses information security policy objectives and strategies. They agree to the roles and responsibilities for information security across the enterprise as defined in specific policies. They visibly promote and provide business support for information security initiatives throughout the enterprise. The governance group is formed and led by the information security leader and the group may include representatives from major business units.

Information Security Policies

The Information Security Program Policies and Controls are based on the CIS Controls v8 Implementation Group 1 and select Group 2 and Group 3 Controls. Group 1 incorporates Basic Cyber Hygiene safeguards and creates a strong foundation. Group 2 and 3 controls include select Enhanced and Advanced safeguards.

Implementation Guidance

The policy documents are designed to build upon one another. *Start by implementing the following three cybersecurity safeguards.* These three safeguards are critical to preventing system and account compromise and to enhancing the company's ability to recover from a cybersecurity incident.

1. Backup Data	2. Multi-Factor Authentication	3. Patch Management
1. Establish Automated Backups of Critical Data and System Configuration 2. Test Recovery Processes Quarterly 3. Establish Offsite Backup Location 4. Establish Warm and/or Cold site recovery capabilities for business critical systems	1. Require multi-factor authentication (MFA) for access to any system, unless it isn't supported 2. MFA should be required for all users: Prioritize users as follows ○ Privileged Users ○ Administrative Users ○ Remote Access Users	1. Enable automatic updates 2. Test and deploy patches quickly. Schedule frequency based on CVSS v3.x scoring. Critical and High vulnerabilities should be prioritized based on system impact 3. Replace unsupported operating systems, applications, and hardware

Implementation of these three safeguards requires a detailed understanding of the Information Technology Environment (Hardware, Software, User Accounts, Network Architecture, Cloud Services, etc…). WEC Group Ltd should perform a risk assessment to determine the potential impact a cybersecurity incident could have on its Information Technology Systems.

The policies and controls do not dictate how the safeguards are implemented. The people, processes, and technology selected to satisfy the policy and control requirements is the responsibility of the Information Security Leader. A risk assessment will inform the Information Security Leader of the potential business impact a cybersecurity incident could cause, and aid in the prioritization and deployment of any resources required to implement the policies.

Policies and Guidelines

The following policies establish "management's intent" for cybersecurity and data protection requirements that are necessary to support WEC Group Ltd's overall strategy and mission:

- *IS.02 Basic Cyber Hygiene Policy* - Controls that must be implemented regardless of risk.
- *IS.03 Enhanced Cyber Hygiene Policy* - Specific CIS Group 2 controls selected to address increased levels of risk and operational complexity.

- *IS.04 Advanced Cyber Hygiene Policy* - Specific CIS Group 3 controls selected to lesson the impact of sophisticated cyber attacks.
- *IS.05 Cybersecurity Guidelines* - Optional CIS Group 2 and 3 controls that should be implemented depending business requirements.

Control Monitoring Requirements

Specific Policy Controls and Safeguards must be reviewed periodically. The following schedule summarizes these requirements.

Requirement	Daily	Weekly	Monthly	Quarterly	Annual
Audit Hardware and Software Asset Inventory			X		
Security Awareness Training and Knowledge Check					X
Password Update Audit					Bi-Annual
Account Access Control Audit					Bi-Annual
Access Log Retention Audit	Every 90				
Dormant Account Review			X		
Rotate Guest Wireless Access				X	
Vulnerability Scan and Remediation			X		
Review Log Retention				X	
Configure AV/EDR Integrity Checks	X				
Perform AV/Malware Scans		X			
Scan / Monitor Internet Facing Systems and Websites		X			
Security Patch Installation * (C) Critical patches (CVSS 9-10)	(C)*		X		
Audit Physical Access Control Logs				X	
Review and Test Backup Storage Media				X	
Test Disaster Recovery Plan				X	
Review and Revise Incident Response Plan				X	

Test Incident Response Plan					X

Exceptions

While every exception to a policy requirement or control potentially weakens the safeguard for WEC Group Ltd's information systems and underlying data, occasionally exceptions will exist. The Information Security Leader will define the procedure that must be followed when requesting an exception, the approval process, and any audit requirements.

References

1. https://www.cisecurity.org/controls
2. https://www.cisecurity.org/controls/cis-controls-navigator/
3. https://www.cisa.gov/cyber-essentials
4. https://www.nist.gov/cyberframework
5. Vulnerability Databases
    a. https://nvd.nist.gov/vuln-metrics/cvss - National Vulnerability Database | CVSS Scoring Criteria
    b. https://cve.mitre.org - Catalog of publicly disclosed cybersecurity vulnerabilities
    c. https://attack.mitre.org/ - Knowledge base of adversary tactics and techniques based on real-world observations

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