



**CITICORE
RENEWABLE
ENERGY**

HUMAN RESOURCES AND ADMIN

Operational Procedure

IT Cyber Security Policy


Document Code, Rev: 0

Effective Date: May 10, 2023



VERSION HISTORY

Rev. No.	Rev. Date	Description of Change	Author / Originator
0	May 10, 2023	Initial Issuance	Roxanne Kimberley Lacerna

	Name	Position	Signature	Date
Prepared by:	Roxanne Kimberley Lacerna	Jr. Supervisor – Talent Acquisition and Management		05/10/2023
Reviewed by:	Lalaine Rosales	AVP - HRA		
Reviewed by:	Mia Cortez	Chief Finance Officer		
Approved by:	Oliver Tan	President & CEO		

Copyright 2023. Citicore Renewable Energy Corporation. All rights reserved.

No part of this procedure may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Citicore Renewable Energy Corporation.

While every effort has been made to ensure the accuracy of the information contained in this accounting manual, Citicore Renewable Energy Corporation assumes no responsibility for errors or omissions, or for any damages resulting from the use of the information contained herein.

This procedure is intended for internal use only by Citicore Renewable Energy Corporation. employees and authorized personnel. Any unauthorized use, dissemination, or copying of this procedure is strictly prohibited and may be a violation of applicable laws.

1.0 PURPOSE

To ensure that all user complies to Cybersecurity Policy guidelines

- a. Mitigate Cybersecurity risk and threats that could impact the business operations
- b. Protect critical IT infrastructure and system from Cyber attacks
- c. Detect and preempt information security breaches such as misuse of networks, data, applications, and computer systems.
- d. Maintain the reputation of the organization, and uphold ethical and legal responsibilities.

2.0 SCOPE

This document is applicable to the following:

- a. The Company and its employees, including subsidiaries and their employees; and
- b. Third-party entities authorized and engaged by the Company and its subsidiaries in the course of official business.

3.0 DEFINITION OF TERMS

- 3.1 Cybersecurity - is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies.
- 3.2 Cybersecurity Threats - Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.
- 3.3 Phishing - is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
- 3.4 SPAM - any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

4.0 POLICIES

4.1 Web Browsing Security

- 4.1.1 The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for corporate environment. The following protocols and categories of websites should be blocked from the corporate firewall:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Emails like Yahoo and Gmail is blocked and only official company email portal access is allowed.

- 4.1.2 Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative. HR will present all approved exception requests to Information Technology Head in writing or by email. IT will unblock that site or category for that associate only. IT will track approved exceptions and report on them upon request.
- 4.1.3 CREC staff should avoid connecting to corporate intranet websites and logging in their credentials on O365 portal using wifi access from coffee shop, malls, and other public places.
- 4.1.4 In general, IT Department does not recommend using Browser Add-ons and freeware tools, however we do not forbid the use of these tools if they enhance productivity. IT department should be consulted before installation of such Add-ons and should be approved by the IT head.

4.2 Email Security

The email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any employee should report the matter to their supervisor immediately.

4.3 Password Security

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements set on each application. Password should be changed every 90 days.

4.4 Data security

- 4.4.1 All information transmitted from the device must be encrypted by a strong encryption algorithm to minimize the risks of eavesdropping on the communications and man-in-the middle attacks.
- 4.4.2 Users are expressly forbidden from storing data on devices and removable media that are not authorized by IT Department and approved by IT head.
- 4.4.3 CREC staff should not use removable media in their work computers without explicit permission of the IT department. Sensitive information should be stored on removable media only when required in the performance of assigned duties or when providing information required by the government. When sensitive information is stored on removable media, it must be encrypted in accordance with the Acceptable Encryption Policy
- 4.4.4 Sensitive information of CREC should not be shared with an unauthorized individual or external parties. It is the responsibility of CREC staff to safeguard the confidentiality and security of data owned by CREC.
- 4.4.5 All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging history

4.5 Security and Protection of IT Resources

- 4.5.1 It is the policy of CREC that mobile computing and storage devices should be approved and configured by IT department prior to connecting to the information systems and CREC network. This pertains to all devices connecting to the CREC network regardless of device ownership. Unconfigured devices should be connected to public wifi only
- 4.5.2 Laptops must employ full disk encryption with Bitlocker managed centrally by the IT department.
- 4.5.3 Employees should not install software, not authorized by IT department, on the device issued by the company. IT Department will obtain and track the licenses, test new software for conflict and compatibility. Only IT department is authorized to perform the installation on the user's devices. In such cases that a non-standard software is needed by the user in accordance to his task, this should be approved by the immediate manager and IT head.
- 4.5.4 Recommended processes to prevent virus problems:
 - 4.5.4.1 Follow IT security corporate standards
 - 4.5.4.2 Do not open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
 - 4.5.4.3 Delete spam, chain, and other junk email without forwarding,
 - 4.5.4.4 Never download files from unknown or suspicious sources.
 - 4.5.4.5 Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

4.5.4.6 Store critical data on one drive to safeguard and backup the file centrally from the server and do not save it on your personal drive or pc.

4.5.4.7 New viruses are discovered almost every day. Anti-virus program and windows patches on your computer should always be updated.

4.6 Securing Training

4.6.1 CREC staff are required to attend and participate to periodic Cybersecurity training to enhance the employee's competency in combatting and identifying Cybersecurity Threats. This is mandatory to all CREC employees.

4.6.2 Employees competency will be measured thru test and assessment.

4.7 Penalty

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.