Policy Name:	**C-300-2 Data Security and Cyber Security Policy**
Functional Area:	**Corporate**
Purpose:	**To define the structure and requirements of Data Security, Cyber Security & Privacy**
Effective Date/Revision Date:	**September 1, 2-22**
Responsibility:	**Jay Forrester**
Frequency:	**Annual**
Policy	**See attached policy for Distribution**
Prepared By:	Jay Forrester
Reviewed By:	Pallavi Singh
Policy Filename:	C-300-2 GCS Cyber Security
Policy File Location:	Teams/Corporate Policy/Files

GAMECHANGE SOLAR
REPOWERING THE PLANET

Overview

GameChange Solar ("Company") commits to the protection of corporate, customer, and employee data sensitive information with which it is entrusted. This is a foundational enterprise principle that governs our actions and digital activities in how we innovate and build world-class solar solutions and how we protect our customer, our company, our people and our business partners.

Maintaining security of Company's data private data of its employees, Intellectual Property as well as protecting against cyber criminals is a top priority of the Company. As criminal techniques become more sophisticated and geopolitical threats emerge worldwide, the need for 24/7 threat detection, investigation, and immediate remediation becomes a requirement and not a luxury. Legacy policies that depend on employees and their front line to notify up chain upon suspicion of a breach are no longer sufficient.

Requirements

It is the policy of the Company to maintain a top tier 24/7 threat detection, investigation, and remediation service for all endpoints on its network infrastructure. This will ensure the protection and privacy of corporate, customer, and employee data including payroll sensitive information.

SOC Compliance

GCS is SOC (Security Operations Center) compliant and hires a vendor that supplies a SOC service providing a team of security analysts that monitor network traffic to and from all company network endpoints for potential threats. Upon threat detection, and investigation into the threat and immediate remediation will occur if needed. This is a 24/7 365 service.

Threat Notification

The SOC vendor will notify GCS upon detection of a potential threat and after an initial investigation to prove it valid. This notification will be made immediately to the CFO and Director of IT. Dissemination of information to other leadership and staff will be determined and executed according to needs of remediation and overall response.

Network Endpoints

Every networked device on Company's infrastructure represents a potential doorway for a cybercriminal. IT department installs special security software that constantly reports information back to the SOC Service for analysis.

A network device can only be modified by the IT department, as it is critical from security standpoint that all endpoints are covered by having the security software installed and running.

Enforcement

All employee laptop and desktop computers will have the endpoint security software installed and always running.

Any employee that violates this policy by refusing to have it installed or attempting to tamper with the software in any way that may render it ineffective, may be subject to disciplinary action up and including termination of employment.