# Ecological Estates Information Technology Security Guidance

## Table of Contents

## Purpose

Ecological Estates views the security of company, client and supplier data as integral to carrying out the mission of the company. The company will develop documented comprehensive awareness programs, plans, and policies for ensuring the security of all data related to the business of the company.

This document is to define the general guidelines established by Ecological Estates, to provide employees and contractors with the best practices for securing company, client and supplier data.

## Terms

**Computer** – Any personal computer that is used to transfer company information within the company or to outside clients or suppliers.

**Mobile Device** – Cell phone, tablet or any handheld portable device that is capable of communicating through the internet via cellular carrier network or Wi-Fi network.

**Home Network** – Any local area network (LAN) set up for home or small office use.

**Incident** - An incident is any one or more of the following:

- Loss of information confidentiality (data theft)
- Compromise of information integrity (damage to data or unauthorized modification).
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Misuse of services, information, or assets.
- Infection of systems by unauthorized or hostile software.

**Data:** Any form of information that contains company, client, or supplier information.

## Access

Only users authorized by the company will have access to company, client or supplier data. No person is authorized to access company, client or supplier data without the written approval of the CEO or COO of the company.

The CEO or COO has the right to revoke access to company data at any time.

# Data Security Protection

## Passwords

- Personal passwords for company related accounts will be at least 8 characters long and will use a combination of uppercase, lowercase, numerical and special characters. Avoid personal information (SSN, birthdates, addresses, etc.) and dictionary words for maximum protection.
- Passwords and usernames will not be shared with the exception of specific role based accounts approved by company management.

## Electronic Mail (e-mail)

Avoid using personal email accounts for transmitting company, client or supplier information. Use the company assigned email account whenever possible.
Never allow anyone other than you access to your company email account.

## Personal Computers

Computers will be password protected.
Unattended computers should be locked to a permanent object when unattended in a public accessible space.
Computers will have up to date anti-virus protection.

## Networks

Any Wi-Fi network used to transmit or communicate company data from a computer or mobile device will be protected by AES encryption or stronger. Do not use an unprotected or WEP (Wired Equivalent Privacy) protected network.
A good rule of thumb is that if a network does not require an access password, do not use it for company business.

## Mobile Devices

Mobile devices should not be used to transmit company data when possible. Avoid storing any confidential information on mobile devices.
Mobile devices that contain any company related data will be password protected.

# Information Security Incident Response

## Incident Response Team

The CEO or COO of the company will be responsible for assembling and leading the incident response team immediately upon identification of a security incident. The team's responsibility will be to:

- Determine the scope of the incident
- Determine the impact of the incident
- Determine the plan for containment, mitigation and corrective action.
- Document the incident and resolution.

## Incident Response

The goals of incident response is to:

- Verify that an incident occurred.
- Maintain or restore business continuity.
- Reduce the incident impact.
- Determine root cause of the incident.
- Prevent future attacks or incidents.
- Improve security and incident response.
- Prosecute illegal activity.
- Keep appropriate stakeholders informed of the situation and response.

## Incident Communication

- Incidents and the incident response will be documented for internal use.
- The incident response team leader will determine the appropriate communication based on scope. The following communication will be considered:
  - Employees
  - Contractors
  - Clients
  - Suppliers
- The proper law enforcement authorities will be notified if unlawful activity has been identified.