ISSP on use of company computers & networks for *Verdant Delights, Inc.*

1. STATEMENT OF PURPOSE

a. Scope and Applicability

Every user of the computers and networks at Verdant Delights Inc.

b. Definition of Technology Addressed

This ISSP is focused on using company computers and networks, specifically non-organizational computing equipment and organizational computer equipment.

c. Responsibilities

It is the responsibility of all management to ensure that these policies are being implemented and enforced. While the responsibility of following these guidelines is given to all users of the network, regardless if they are hired by this company or not.

2. AUTHORIZED USES

a. User Access

General internet and computer access is permitted to those who adhere to these guidelines and uphold them on company and personal devices.

b. Fair and Responsible Use

Users must use this network or these devices only for business or authorized objectives, and not for personal or illegal activities.

c. Protection of Privacy

Verdant Delights, Inc. must adhere to the General Data Protection Regulation law with diligence and care, ensuring that all users of this network have their privacy and information protected before, during, and after transmission of this information.

3. PROHIBITED USES

a. Disruptive Use or Misuse

Viewing of any sort of inappropriate media or websites. Downloading files that are not authorized or with business purposes. Sending or viewing personal emails not associated with work.

b. Criminal Use

Unauthorized use of local network analysis tools such as Wireshark or tcpdump. Downloading malware or software that could potentially harm company devices or the network. Sending malicious emails.

c. Offensive or Harassing Materials

Offensive or harassing materials include the display of pornographic images, hate symbols, violent images, or degrading images, on any devices that are in the vicinity.

d. Copyrighted, Licensed, or Other Intellectual Property

All copyright or licensing follows under the guidelines set by the Fair Use Policy of the U.S. Copyright Office.

e. Other Restrictions

Sites that are not in use of Hyper Text Transfer Protocol Secure are not permitted for the purpose of protecting user information from a lack of encryption.

4. SYSTEMS MANAGEMENT

a. Management of Stored Materials

Information will be reposited, and backed up through the various systems and backups located at Verdant Delights, Inc. All of which will be using end-to-end encryption.

b. Employer Monitoring

Verdant Delights, Inc. May monitor computer activity on the network and computers for any purposes including, but not limited to: investigation in incident response and event management.

c. Virus Protection

All company devices must have the Endpoint Protection Service Crowdstrike Falcon to ensure device and network safety, and to be free from common threats and viruses.

d. Physical Security

These systems will be protected by being located in Room 127, which is guarded by the requirement of access to the IT Manager's room at Room 126.

e. Encryption

The encryption in place will be Advanced Encryption Standard 256 for its robustness and modern security.

5. VIOLATIONS OF POLICY

a. Procedures for Reporting Violations

Issue Specific Security Policy violations are to be disclosed to the IT Manager, Celica Thompson either via email or an anonymous reporting channel that is provided by the organization.

b. Penalties for Violations

Potential termination, civil or criminal penalties, and disciplinary action at a minimum, will be met to those who violate this policy.

6. POLICY REVIEW AND MODIFICATION

a. Scheduled Review of Policy

A survey on this ISSP should operate annually, to ensure that this policy never reaches an obsolete state, and will remain effective.

b. Procedures for Modification

The procedure of modifying this policy starts with identifying what specifically needs to be adjusted or addressed. Next, implement a solution for this adjustment that ensures that either the policy remains as secure, or more secure than it was before.

7. LIMITATIONS OF LIABILITY

a. Statements of Liability

Any violators of this policy are responsible for any damage, loss, or infringement on property that comes from the use of the company's network. Users of the network are responsible for adhering to this policy to ensure that no damage is done to the network and its assets. Any violation of this policy will result in rejection of continuing the service provided, and if harm is done, compensation will be demanded.

b. Other Disclaimers

This business may be held responsible for damages if the damage occurs without any immediate and identifiable user found being responsible. Violators of this policy may potentially infringe upon the Computer Fraud and Abuse Act in the process of violating this policy.

REFERENCES

(n.d.). General Data Protection Regulation (GDPR) – Legal Text. Retrieved November 10, 2025, from https://gdpr-info.eu/

CrowdStrike. (2025). *The Agentic Security Platform. Unified and build to secure the AI revolution*. Crowdstrike. https://www.crowdstrike.com/en-us/platform/

A Guide to U.S. Cybersecurity Laws and Compliance. (2024, December 5). NRI Secure. Retrieved November 10, 2025, from https://www.nri-secure.com/blog/us-cybersecurity-laws-compliance#TOC_HL3

U.S. Copyright Office. (2025). *U.S. Copyright Office Fair Use Index*. U.S. Copyright Office. https://www.copyright.gov/fair-use/