Hortech's Information Technology Standard	No: v25-006
IT Standard: **Acceptable Use of Information Technology Resources Policy**	Updated: 07/01/2025
	Issued By: Human Resources Owner: Jon Eberly, IT Manager

1.0 Purpose and Benefits

Appropriate organizational use of information and information technology ("IT") resources and effective security of those resources require the participation and support of the organization's workforce ("users"). Inappropriate use exposes the organization to potential risks including virus attacks, compromise of network systems and services, and legal issues.

2.0 Authority

This policy is issued under the authority of Hortech's General Management and Information Technology Management. They are responsible for overseeing the implementation, adherence, and periodic review of this policy to ensure it remains relevant and effective. The policy must be adhered to by all users of the organization's IT resources to maintain the security and integrity of the organization's information and systems.

3.0 Scope

This policy applies to users of any system's information or physical infrastructure regardless of its form or format, created or used to support the organization. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organization's Information Security Policy and its associated standards.

4.0 Information Statement

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the organization's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner including in real-time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems, and other electronic records). In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the organization's IT resources is not permissible.

The organization may impose restrictions, at the discretion of their general management, on the use of a particular IT resource. For example, the organization may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the organization's IT resources (e.g., personal USB drives, cellphones).

Users accessing the organization's applications and IT resources through personal devices must only do so with prior approval or authorization from the organization.

4.1 Acceptable Use

All uses of information and information technology resources must comply with organizational policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws. Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting organizational information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;

- Observing authorized levels of access and utilizing only approved IT technology devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Information Technology Department.

4.2 Unacceptable Use

The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities, after approval from organizational management, in consultation with organization IT staff (e.g., storage of objectionable material in the context of a disciplinary matter). Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of organization information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Attempting to represent the organization in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the organization's network or any IT resource;
- Connecting organizational IT resources to unauthorized networks;
- Connecting to any wireless network while physically connected to the organization's wired network;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with organizational policies;
- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (organizations must recognize the inherent risk in using commercial email services as email is often used to distribute malware);
- Using an organization's IT resources to circulate unauthorized solicitations or advertisements for non-organizational purposes including religious, political, or not-for-profit entities;
- Providing unauthorized third parties, including family and friends, access to the organization's IT information, resources, or facilities;

- Using organizational IT information or resources for commercial or personal purposes, in support of "for-profit" activities, or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using organizational IT resources; and
- Tampering, disengaging, or otherwise circumventing an organization or third-party IT security controls.

4.3 Occasional and Incidental Personal Use

Occasional, incidental, and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the organization's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. Organizations may revoke or limit this privilege at any time.

4.4 Individual Accountability

Individual accountability is required when accessing all IT resources and organizational information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system and protecting your credentials (e.g., passwords, tokens, or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared.

4.5 Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted organization, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a

personal email account to conduct the organization's business unless explicitly authorized. Users must not store restricted organizational, non-public, personal, private, sensitive, or confidential information on a non-organizational issued device, or with a third-party file storage service that has not been approved for such storage by the organization. Devices containing organizational information must be attended or physically secured.

4.6 User Responsibility for IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the organization and must be immediately returned upon request or at the time an employee is separated from the organization. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the organization.

- Should IT equipment be **lost** or **broken** due to negligence, users will be required to reimburse the organization for the replacement value of the equipment through **payroll deduction**.
- In the case of **accidental damage**, the IT department will evaluate whether reimbursement is required based on the circumstances.
- All incidents involving **lost or broken equipment** must be immediately reported to the IT Department to facilitate replacement.

No employee is permitted to independently purchase replacement equipment. Any unauthorized purchases will not be reimbursed, and employees must rely on the organization's approved procurement processes. Any unapproved equipment is not authorized to be used.

Employees who repeatedly lose or damage IT equipment may face disciplinary action, and the organization reserves the right to not issue or re-issue IT devices and equipment to these individuals.

4.7 Cybersecurity Training Compliance

Users are required to complete assigned cybersecurity training as part of their responsibility to understand and implement baseline information security controls. This training equips users to recognize and respond to potential threats, such as phishing attempts, malware, and other cybersecurity risks. Timely completion of these trainings is mandatory and monitored, as specified in Hortech's Acceptable Use Policy.

Failure to complete assigned training may result in disciplinary actions, including but not limited to:

- Notification to the employee's manager.
- Documentation of non-compliance in a professionalism review.
- Documentation of non-compliance in an appraisal.
- Temporary suspension of access to non-essential IT resources until training is completed.
- Escalation to Human Resources for further investigation and disciplinary action.

- Temporary reassignment or suspension from sensitive duties requiring cybersecurity awareness.
- Revocation of remote work privileges or personal device access to organizational systems.
- Termination of employment for repeated and unresolved non-compliance.

These measures are designed to ensure accountability and reinforce the importance of cybersecurity awareness in safeguarding Hortech's organizational security and resources.

5.0 Use of Social Media

The use of public social media sites to promote organizational activities is restricted to selected individuals.

Acceptable Use:

- Promoting organizational events and activities with pre-approved content.
- Sharing industry news and developments relevant to the organization.
- Responding to public inquiries in a professional and approved manner.

Unacceptable Use:

- Posting unauthorized or confidential information about the organization.
- Sharing offensive, discriminatory, or inflammatory content.
- Using organizational social media accounts for personal purposes.

Guidelines for Personal Use of Social Media:

- Conduct yourself in a responsible, professional, and secure manner.
- Do not post identifying information of staff without permission.
- Use disclaimers when expressing personal views that could be construed as official communications.
- Do not use personal social media accounts for official business unless specifically authorized.
- Avoid using the same passwords for personal and organizational accounts.

6.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time. If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through General or IT Management.

6.1 User Acknowledgment and Implied Consent

By accessing or using any Hortech IT resource—including but not limited to computers, email, mobile devices, systems, applications, or networks—users acknowledge that they have read, understand, and agree to comply with this Acceptable Use Policy.

Use of Hortech's IT systems constitutes implied consent to the monitoring, auditing, and enforcement practices described herein. If a user does not agree with the terms of this policy, they must immediately cease use of all Hortech-provided IT resources and notify their manager or the Human Resources Department.

7.0 Definitions of Key Terms

Term	Definition
Confidential Information	Any information that is intended to be kept secret and is only shared with a limited number of people who need to know it for their job. This includes, but is not limited to, personal data, financial information, proprietary information, and trade secrets.
Information Technology (IT) Resources	Includes all computer systems, networks, software, data, and related equipment owned, leased, or operated by the organization. This also encompasses internet access, email, and any other IT services provided by the organization.
Personal, Private, and Sensitive Information (PPSI)	Information that is protected by privacy laws and regulations. This includes personal data such as social security numbers, financial data, health information, and other sensitive personal information.
Privileged Accounts	Accounts with elevated access rights, typically used by IT staff or other authorized personnel to manage systems and applications. These accounts can perform a wider range of activities compared to regular user accounts.
Social Media	Online platforms and tools that allow users to create and share content, and to participate in social networking. This includes but is not limited to, Facebook, Twitter, LinkedIn, Instagram, YouTube, and mass emailing platforms used for distributing content to large groups of recipients.
Unauthorized Use	Any use of IT resources that is not explicitly approved by the organization or that violates organizational policies, standards, procedures, or guidelines.
User	Any individual who uses the organization's IT resources. This includes employees, contractors, consultants, temporaries, and other workers at the organization, including all personnel affiliated with third parties.
The Organization	Hortech and its subsidiarys (including but not limited to LiveRoof, LiveRoof Global, LiveWall, Norb Lighting, and SteadFast Shipping)

8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Human Resources Department Email: alicia@hortech.com
Phone: 616-935-1966

To report any malicious activity, suspected security incidents, or any activity referenced in this policy, please contact:

Information Technology Department Email: infosec@hortech.com
Phone: 616-935-1977

General Management Email: davem@hortech.com
Phone: 616-935-1965

Reports can be made anonymously, and all reports will be handled with the utmost confidentiality to protect the reporter's identity and ensure thorough investigation and resolution.

9.0 Revision History

This policy shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
11/08/2024	Initial Version Created	Jon Eberly
07/01/2025	Included new section 6.1	Jon Eberly