USUI INTERNATIONAL CORPORATION
Electronic Systems Policy

1. Electronic Communications Purpose

Usui International Corporation ("UIC") maintains electronic systems including but not limited to computers, computer networks, electronic mail systems, internet, telephones, cellular phones, and voicemail systems ("Electronic Systems"), to assist in communications and to conduct business.

Because these Electronic Systems are its property, UIC has the right to monitor, access, review and disclose, at any time, any message or document created, received, or sent using these Electronic Systems, including any incidental personal usage.

These Electronic Systems should be used principally for business purposes. Employees should not use the Electronic Systems for personal use such as searching the internet or sending email with a personal account. These policies apply to all employees of UIC.

2. Acceptable Use of Electronic Systems

UIC strives to maintain a workplace that is free of harassment and that is sensitive to the diversity of its employees. Therefore, UIC prohibits the use of its Electronic Systems in ways that are illegal, disruptive, offensive, discriminatory, harassing, or harmful. Prohibited use includes the display or transmission of messages that contain sexually explicit or offensive images or statements, racial slurs, or any other comments that address someone's gender, age, sex religion, national origin, creed, disability, sex orientation or gender identify or any other legally protected characteristic in an offensive, discriminatory, or harassing manner.

Although UIC has little control over inbound electronic messages, employees should avoid passing on inappropriate messages or images. Employees should also notify senders to refrain from sending messages with inappropriate content.

In addition, UIC's Electronic Systems may not be used in a manner that violates copyrights, patents, license agreements, and/or proprietary constraints. Moreover, UIC's Electronic systems may not be used to disparage UIC or its customers, vendors, or employees.

3. Approved Equipment

UIC information should only be stored on company-owned devices (computers, DFS network) or company-supported sites (Plex, Adaptive Insights, ADP, Fidelity). General guidelines are as follows:

- All important documents should be stored in UIC Teams or DFS locations.
- Other documents can be stored in OneDrive/Documents.
- No UIC information should be stored in unapproved devices such as flash drives or sent to a personal email account.
- Reasonable care should be exercised to protect portable devices such as laptop computers.

4. Data Classifications

All information that is not publicly disseminated is considered confidential. Confidential information includes the following:

- Financial Information- Includes financial statements, tax returns, confidential correspondence. etc.
- Personal information – Includes individual's names, family member's names, tax identification numbers, compensation, medical records, birthdays, passport numbers, visas, bank account numbers, credit card information, etc.
- Protected Health Information – Includes health information, health care provider, health plans, medical or mental health issues, etc.
- Proprietary Information – Includes pricing, sales contracts, patents, drawings, blueprints, purchase agreements, production plans, manufacturing processes, etc.

5. Protection of Confidential Information

UIC uses the following methods to protect confidential information

- Physical Access – Protection includes access systems, security cameras, locked files, etc.
- Electronic Access – Individuals are granted limited access after password authentication to information based upon the nature of their position.
- Nondisclosure agreements – For employees, both the Employee Handbook and Employee Code of Business Ethics and Conduct prohibit the disclosure of confidential information. For on-site visitors, nondisclosure agreements must be signed.
- Mobile Device Management – Allows for the remote removal of information from a mobile device.
- Internet Access – UIC provides both network and guest wi-fi access. When out of the office, employees should avoid public internet such as hotels and airports.

6. Access and Authentication Controls

Access to UIC networks and workstations is achieved through individual authentication with user identification and complex password.

- Employees must always protect passwords. Passwords should never be shared with another person, written down in an easily accessible place, or recorded in an unsecured device.
- Employees should never leave a workstation unattended and unlocked. The network will lock a workstation after a period of inactivity.
- Administrators will periodically require employees to change passwords.
- Employees should immediately change a password if there is chance it has been compromised.

UIC provides both network and guest wi-fi networks.

- Visitors should only be given access to the guest wi-fi network.
- Employees are not allowed to connect devices for personal use.

7. E-Mail

The following precautions should be followed:

- UIC Email can only be downloaded on a company-owned computer or cellular phone with Mobile Device Management. UIC e-mail should NEVER be placed on a personal cellular phone.
- Caution should be used when sending or receiving confidential information. When possible, precautions should be taken to protect the data (share link from OneDrive/Teams or Encrypt).
- UIC maintains an archive of all in-coming and outgoing email.

8. Cellular Phones

A company-provided cellular phone will be issued to eligible employees.

- Examples of factors used to determine eligibility include those in a position that require
  - Frequent travel
  - Contact in the event of an emergency
  - Contact during off hours.
  - Immediate availability to meet time-sensitive decisions
  - Remote access to UIC's email.
- The IT department negotiates, maintains, and manages the approved cellular phones based upon cost, features, security, and support. The IT staff will only support a limited number of models.

- All company-provided cellular phones must have a Mobile Device Management system installed. This will allow for a phone to be remotely wiped.
- Only exempt employees are eligible for a company-provided cellular phone with UIC email.
- Periodically, managers will reassess an individual's needs for a company-provided cellular phone.
- Employees should always comply with local, state, or federal law when using a cellular phone.
- Employees should always avoid distracted driving. An employee should never read or send text/email messages while driving.
- Employees should use a company-owned device prudently, limiting the amount of data and roaming charges incurred.

9. Virus and Malware Protection

UIC monitors virus/malware activity on all devices through anti-virus/malware software which is enabled and regularly updated.

- Employees should not disable or circumvent anti-virus/malware systems installed to protect UIC.
- In the event of a suspected virus/malware infection, employees should immediately inform the IT staff. Do not forwarded a potentially infected file.
- Willfully or recklessly introducing computer viruses, malware, as well as disruptive or destructive programs into the UIC environment is prohibited.

10. Software Use

Employees may only use the software on the company-provided computers and networks.

- UIC recognizes the importance of copyright and other protections afforded to the creators of intellectual property. Employees are responsible for making use of software and other information technology resources in accordance with copyright and licensing restrictions.
- Using information technology resources in a manner violating these protections or furthering the unauthorized use or sale of protected intellectual property is prohibited.
- UIC purchases and licenses the use of various computer software for business purpose and does not own the copyright. Unless authorized by the software developer or licensor, UIC does not have the right to reproduce such software for use on more than one computer.

- UIC prohibits the illegal duplication of software and its related documentation.
- Only the IT staff should install software on a company-owned device.
- The use of instant messaging systems other than the UIC-provided system is prohibited.

11. System Monitoring

UIC provides numerous technology related information systems for use on UIC business. UIC reserves the right to monitor all communications and data on its information systems at any time, with or without notice.

- UIC may access and disclose all data or messages stored on its information systems. UIC also reserves the right to disclose the content of these communications and data for any purpose at its sole discretion.
- Additionally, UIC reserves the right, with or without notice, to audit company-owned devices for acceptable use and compliance with these procedures.

12. Loss of Company-Owned Device or Notice of Security Weakness

In the event a security breach, it is critical to immediately report the problem.

- If a device is lost or stolen, the employee must immediately open a ticket in the IT Support system. If after hours, the employee should call or text an IT staff member.
- For potential security weakness, cyber-attack, phishing email, malware notifications, suspicious persons seeking access, or any other activities that may put computer systems or data at risk, an employee is require to report this observation immediately to the IT staff through the IT Support system.
- If a password may be compromised, the employee should immediately change the password and notify the IT staff through the IT Support system.

13. Purchasing of Information System Resources

All information systems hardware and software should be approved for purchase by the IT Department.

- Departments should consult the IT department for assistance and approval of specifications and supplier **before** submitting purchase orders.
- Licensing, copyrights, contract terms, etc. must be accessed regarding legality and optimum structure in conjunction with all UIC locations.

14. Return of Property upon Termination

All UIC property, including the Electronic Systems, user IDs, and passwords discussed above, must be returned to UIC upon termination of employment.

- UIC's policy does not permit the transfer of UIC information to a personal account or device.
- In the event UIC discovers such unauthorized transfers after employment ends, UIC will require such information be deleted or returned on an appropriate device. UIC may require, at such departed employee's expense, third-party verification, acceptable to the UIC, that the UIC's data has been properly deleted.

15. Policy Violations

Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

- Because of the importance of our data and information security systems, UIC employees acknowledge their agreement to comply with this policy at the time of hire and annually thereafter.
- Employees should notify the IT Staff through the IT Support system upon learning of violations of this policy.
- Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment. In the event of a lost or stolen device, additional disciplinary action may include reimbursing UIC for replacement cost of the lost or stolen equipment.
- UIC reserves the right to update and modify this policy as needed. Employees will be notified of any changes to this policy. It is the employee's responsibility to review and comply with all updates, including electronic updates to these procedures.

Usui International Corporation
Acknowledgement

I have received a copy of the Usui International Corporation Electronic System Policy. I understand that it is my responsibility to read and comply with the guidelines contained in the policy. Violations of this policy are subject to disciplinary action, up to and including termination. I also understand and accept the fact that any guideline in the policy are subject to change at the sole discretion of the Company at any time.

_____

(Signature of Employee) (Date)

_____

(Printed Name) (Title)