DATA SECURITY POLICY FOR EMBEDDED SPECIALTIES, INC

BACKGROUND

Today's organizations are challenged to foster a productive work environment while securing both their network and their data. As technology continues to advance and data regulations evolve, ESI must help its employees understand their role in data security. This policy outlines how employees should be interacting with ESI's IT systems and data.

PURPOSE

It is essential for ESI to safeguard restricted, confidential or sensitive data from theft, leakage or any other type of infringement, so as to prevent detrimental outcomes like reputational damage, productivity loss or regulatory repercussions. ESI's Data Security Policy is designed to reflect the organization's dedication to manage all information, including that of employees, customers, stakeholders and others, according to strict standards of confidentiality and care. The policy's goal is to ensure that data is gathered, stored and handled in a manner that honors individual rights and protects all parties from any harm caused by the misuse of data or IT systems.

SCOPE

This universal company policy refers to any person or party who uses ESI's data or systems in any way, including employees, vendors, stakeholders, consultants, contractors, etc. It includes anyone we collaborate with or who acts on our behalf and may need access to our data, such as but not limited to:

- Financial Information
- Personally identifiable information
- Sensitive or confidential data
- Login credentials and passwords
- Critical business assets

In cases where any aspect of this policy affects areas governed by local legislation, local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. Employees of ESI who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

DEFINITIONS

The term "users" refers to any and all individuals who have access to any of ESI's IT systems. It includes but is not limited to employees, stakeholders and outside parties. The term "IT systems" refers to any and all equipment that connects to the corporate network or that accesses corporate applications. It includes but is not limited to computers, laptops, smart devices, printers, data and voice equipment and networks, software, electronically stored data, portable data storage devices and video conferencing systems. The term "personal information" refers to information concerning an individual that is considered non-public information including but not limited to health, financial or medical information including electronic medical records, social security numbers, financial or bank account information, driver license numbers, credit card numbers and e-mail addresses.

POLICY DETAILS

ESI's systems exist to support and enable the organization. It should not be employed for personal use, especially if such use impedes productivity or results in any direct costs to ESI.

DATA SECURITY POLICY FOR EMBEDDED SPECIALTIES, INC

ESI reserves the right to monitor the use of its data and systems at any time, as well as to regularly audit networks and systems to ensure compliance with this policy.

ESI must collect and process data as part of our operations. All users must ensure that this data is accurate, up-to-date, managed lawfully and protected against any unauthorized or illegal access by internal or external parties.

Any data obtained and/or managed by ESI must not be communicated informally, stored for more than a specified amount of time, transferred to other parties that do not have adequate data protection policies or distributed to any party other than the ones agreed upon by the data's owner (except legitimate requests from law enforcement authorities).

Only smartphones, tablets and similar devices controlled by an approved mobile device management policy will be allowed to access ESI's IT system, including e-mail, printers and other devices.

ESI must inform people of how their information is being collected, processed and accessed, and allow them to request modifications, deletions or corrections to that data.

Any information that is particularly sensitive or vulnerable, including personal information, must be encrypted and/or securely stored to prevent unauthorized access. In addition, all users must enforce all necessary protocol to minimize unauthorized access to confidential information.

Users are not permitted to send, upload, remove or otherwise transfer any confidential information except where explicitly authorized to do so in the performance of their regular duties.

Users are required to keep passwords secure and not allow others to access their accounts.

Users who are supplied with computer equipment by ESI are responsible for the safety and care of that equipment, as well as the security of software and data stored on it and on other ESI systems that they can access remotely using it. Users must immediately notify the IT team in the event that a device containing sensitive data is lost.

All ESI workstations must be set to automatically lock after 10 minutes of inactivity, and every user is required to manually lock their machine whenever leaving it unattended.

All ESI devices will be configured to automatically download and install the latest manufacturer's updates and/or patches. For devices where this is not possible or practical, a manual, periodic assessment will be performed and updates/patches will be applied as required.

Users must be trained on and take all necessary measures to guard against the risk of malware infecting ESI's systems, and they must report any actual or suspected malware infection immediately.

No user is permitted to circumvent ESI's implemented security systems or protocols or to use any software or applications that are not approved and monitored by our IT team.

All employees, upon onboarding, will be required to sign documentation that confirms they will return all records, in any format, containing personal information to ESI in the event that they are terminated.

DATA SECURITY POLICY FOR EMBEDDED SPECIALTIES, INC

All ESI workstations will be set to automatically backup daily to on-site storage devices. Daily backups will be stored in an encrypted format and the backup data sets will be securely erased once an approved duration has elapsed.

Physical access to servers and storage devices containing sensitive or personal information will be restricted to authorized users.

All active project data will be stored on local servers in an unencrypted format. As required, these local servers will be isolated from one another using commercial firewall devices. Only ESI workstations authorized to access specific projects will be allowed to access specific, isolated servers.

Redeploying, decommissioning or disposing of any storage devices containing sensitive or personal information will be performed by authorized personnel only, using industry accepted procedures or utilities to ensure sensitive or personal information is securely erased prior to being redeployed, decommissioned or disposed.

All paper records containing sensitive or personal information will be shred prior to disposal.

All contracts with third party providers will provide for indemnification of ESI for the unauthorized use or disclosure of stored personal information on their network.

When accessing ESI's network from an off-site location, commercial VPN solutions must be used.

SUMMARY

In accordance with ESI's commitment to data security, we will make every reasonable effort to execute the following actions and procedures:

- Train all employees on their responsibility to uphold the provisions of this policy
- Develop secure networks capable of protecting our systems and data from cyber attacks
- Restrict and monitor access to sensitive data
- Employ security defenses in the form of software, applications or other technological means, and keep them fully up-to-date
- Develop transparent data collection procedures
- Create and communicate clear procedures for reporting privacy breaches or data misuse

DISCIPLINARY CONSEQUENCES

All rules and principles communicated in this policy must be strictly followed. ESI will not tolerate any misuse of its data and/or systems and will discipline any individual found to be in violation of the policy, including termination of employment if deemed necessary. A breach of data security and IT compliance guidelines may also invoke legal action.

DATA SECURITY POLICY FOR EMBEDDED SPECIALTIES, INC

EMPLOYEE ACKNOWLEDGEMENT

I have read and been informed about the content, requirements, and expectations of the Data Security Policy for Embedded Specialties, Inc. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my employment and my continuing employment at Embedded Specialties, Inc.

I understand that if I have questions, at any time, regarding the Data Security Policy, I will consult with my immediate supervisor or my Human Resources staff members.

Please read the Data Security Policy carefully to ensure that you understand the policy before signing this document.

Employee Signature: _____

Employee Printed Name: _____

Receipt By: _____

Date: _____