Silver Blaze Ltd

Silver Blaze Cyber Security Policy

Introduction.

The risk of data theft, scams and security breaches can have a detrimental impact on a company's systems, technology infrastructure and reputation. As a result, Silver Blaze has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose.

The purpose of this policy is to (a) protect Silver Blaze's data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

Scope.

This policy applies to all of Silver Blaze's permanent employees, subcontractors and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data.

Silver Blaze defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Device Security.

Company Use.

To ensure the security of all company-issued devices and information, Silver Blaze employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices password-protected.

- Refrain from sharing private passwords with coworkers or personal acquaintances.
- Regularly update devices with the latest security software.

Personal Use.

Silver Blaze recognizes that employees may be required to use personal devices to access company systems. To ensure company systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

Email Security.

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software. Therefore Silver Blaze requires all employees to:

- Verify the legitimacy of each email.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact a manager regarding any suspicious emails.

Transferring Data.

Silver Blaze recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to the Silver Blaze Data Protection Policy

- Immediately alert a line manager of any breaches, malicious software, and/or scams.

Disciplinary Action.

Violation of this policy can lead to disciplinary action, up to and including termination. Silver Blaze's disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

This policy will be reviewed annually from implementation.

Ciaran O'Duffy

Managing Director 28.06.24