Cryptography Security Policy

This Policy states the Company's intent to use cryptography and web filtering to protect the confidentiality, integrity and authenticity of sensitive, confidential or secret information and sets out how information should be protected by encryption when it is being accessed, transferred or stored.

Introduction and Scope

To protect the confidentiality, authenticity, or integrity of information by the use of cryptography. To avoid breaches of the Data Protection Act and other statutory, regulatory or contractual obligations.

This policy applies to managers with responsibility for the provision of information systems and staff who handle sensitive information through employment. It also applies to third parties who handle sensitive information on behalf of the Company.

Sensitive information comprises information assets that are classified as restricted or secret under the Information Handling Policy and all instances of Protected Personal Information.

This policy applies to sensitive information held on approved Company systems.

Policy

Secure authentication technologis and procedures and cryptographic controls shall be applied according to the sensitivity of the data as defined in the Information Handling Policy.

Sensitive information in electronic form shall only be physically taken for use away from the Company in an encrypted form, unless its confidentiality can otherwise be assured.

The strength of the authentication is appropriate for the classification of the information to be accessed. Where strong authentication and identity verification are required, authentication methods additional to the password are used – such as multi factor authenicatiors or the use of biometrics (fingerprint or a facial recognition scan). Secure remote access and geolocation tracking to safeguard access is in place for all relevant company devices.
The company applies monitoring policies for all staff and completes regular security audits and testings.

- Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.
- The confidentiality of sensitive information being stored on systems outside the Company, or across networks must be protected by use of appropriate encryption techniques.
- Encryption shall be used whenever appropriate on all remote access connections to the Company's network and resources that have the potential to transfer sensitive information (particularly credentials).
- A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, shall be established.
- Staff should not share or display sensitive information or applications with anyone not autorised by the Compnay and then only after log-on process have been successfully completed.
- Staff should not display a password in clear text when it is being entered whenever possible.
- Important business information being communicated electronically shall be authenticated by the use of digital signatures; information received without a digital signature shall not be relied upon.

Web filtering

Web filtering is an essential component of our information security strategies and policies, providing our company with the means to control and secure internet access for our users. By selectively blocking or allowing access to websites and content based on predefined criteria, web filtering helps mitigate security risks, enhance productivity, and enforce compliance with company policies.

The implementation of web filtering involves categorising content, maintaining blacklists and whitelists, and utilizing various filtering techniques such as URL filtering and keyword filtering. Web filtering applies to any company assets, equipment or end point devices.

Prohibited websites:

Prohibiting access to specific websites is a proactive measure to mitigate cybersecurity risks, safeguard sensitive information, and foster a secure digital workspace. The decision to prohibit access to certain websites is typically driven by the need to maintain a secure and productive digital environment while adhering to ethical, legal, and regulatory standards.

These restrictions may include, but are not limited to,

Malicious Websites:

Websites known for hosting malware, spyware, viruses, or other malicious software are prohibited to prevent the spread of infections.

Phishing Websites:

Websites designed to trick users into providing sensitive information, such as login credentials or financial details, are prohibited to protect against identity theft and fraud.

Illegal Content:

Websites that host or promote illegal content, including but not limited to for example child pornography, illegal drugs, or activities that violate local laws, are prohibited.

Hate Speech, Bullying, Discrimination, Harassment and Extremist Content:

Websites that propagate hate speech, bullying, discrimination, harassment or promote violence, or contain extremist content are prohibited to maintain a safe and inclusive online environment.

Proxy and Anonymizer Sites:

Proxy and anonymizer websites that enable users to bypass network restrictions or hide their online activities are prohibited to maintain control over internet usage.

Gambling Sites:

Access to gambling websites is prohibited to prevent potential legal issues or to maintain a focused and productive work environment.

Adult Content:

Access to adult or explicit content is prohibited in workplace environments to maintain a professional atmosphere and comply with workplace policies.

Social Media and Entertainment Sites:

Organizations prohibits personal social media and entertainment websites to minimize distractions and enhance productivity.

Torrent and File Sharing Sites:

Websites that facilitate the unauthorized sharing of copyrighted material, such as torrent sites, are prohibited to avoid legal issues related to intellectual property infringement.

Personal Email and Communication Platforms:

Access to personal email and communication platforms are restricted to prevent data leakage or to ensure that work-related communication is conducted through official channels.

Regular reviews and updates of the list of prohibited websites will be completed, as the digital landscape is dynamic, and emerging threats may necessitate adjustments to the above.

Breaches to the above will result in a disciplinary action.

Related Policies

This policy should be read alongside the Information Handling Policy and other documents within the Company's IT Security Policy.

Policy Review and Assessment

This policy may be amended by Interr at any time in order to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024