fitzgerald & law

Data Security Policy

Introduction

The following describes the Data Security in place from both a virtual and physical perspective and in summary involves:

- Securing the desktop, local password controls, encrypting laptop/external drives and running managed anti-virus protection.
- Ensuring our data is housed on an encrypted platform with full data protection strategy to allow for Visibility, Control and Protection.
- Having cloud access protected by strong password/multifactor authentication (data and email).
- Making sure that phishing, viruses and malware risks are mitigated with and by Office 365 security enhancements supported with next generation firewall and local desktop protection.
- Having data further protected with classification and governance controls – maximising controls and security
- Real time alerting for any breach or risk of a breach.
- Ensuring secure data communication with clients - Outlook encryption, Transport Layer Security (TLS) or secure file sharing.
- Having a robust and effective next generation firewall solution in place.
- Ensuring secure/controlled (and appropriate) access to our physical sites – see below.

Secure file sharing

- Solution is a secure cloud data hosting platform – encrypted at rest.
- Using encryption techniques on all access routes. All data transmission, including uploads, downloads, and browsing is encrypted using 256-bit AES protocol.
- Full data protection strategy – Visibility, Control and Protection of all data.
- Multifactor Authentication (MFA).

Secure communication

- Where possible email is sent through a secure encrypted channel (TLS) which will be configured between our mail servers and the client (requires both sides IT to set this up).
- Outlook Encrypted Messaging to send encrypted communications between each other, this is controlled by either verifying email login credentials or by using a one time passcode.
- Encrypted file share using secure file sharing solution

Security controls in place

- Multifactor Authentication (MFA).
- Local Password security controls – strong password structure, 90 day expiration, history rules and auto lock.
- Device management – controlling devices which access our data, remote wipe or data removal.
- Next generation firewall with real time protection and alerting.
- Protection from ransomware attacks.
- Multiple Layered Protection to prevent virus/phishing/malware and network attacks.
- Controlled access to physical sites as detailed below.

Next generation firewall

- We are using a next generation firewall technology combining traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI) and an intrusion prevention system (IPS).
- This allows for 'real time' notification alerting for any activity around specific types of content (PII) ensuring we are aware of any unauthorised access and able to notify the authorities. Includes threat detection with 'real time' alerting and risk analysis.
- It also allows for Data loss prevention (DLP) – detects and prevents personal identifiable information (PII) from leaving the network.
- Additionally, the NG firewall has web blocker, spam blocker, gateway antivirus and reputation enabled defence to further protect all computers from malware or viruses.

Data classification and governance

- Solution provides a cloud-based content governance solution and effectively protects our employee and customer privacy, intellectual property and confidential information.
- Finds where our sensitive content is and centrally enforces our access policies to maximise control and security.
- In addition, it allows us to manage unstructured data repositories by classifying all of our content and detecting PII (Personally Identifiable information), banking information and any PHI (Personal Health Information) for all European countries and languages.
- Protects from data theft in providing machine learning alerts of any deviation of user patterns i.e. a user logging in from the US then UK within 10 minutes of each other or if a user is set to leave and they suddenly download gigabytes worth of data.
- Allows for real time' notification alerting us to any activity around specific types of content (PII) ensuring we are aware of any unauthorised access to notify the authorities.

Data held in EU

- Email and data in EU hosted datacentres.
- Internal client management software held on our premises encrypted file server.

General security

- Clear desk policy - minimal data files locked away in a secure environment.
- Disaster recovery procedure in place.
- Initial and Annual Penetration testing.
- Controlled access to secure areas and implementation of security and privacy policies with all individuals that have access.
- Working towards Cyber Essential Certificate and EU-US Privacy shield verification.