Camargue

Glossary of Cyber Terms

Biometric Data
A technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

Data Classification Policy
A process of organising data into categories that make it is easy to retrieve, sort and store for future use.

Data Subject
Any natural or juristic person who can be identified, directly or indirectly, via an identifier such as a name, ID number, address etc.

Data Retention and Destruction Policy
A policy that establishes requirements and guidelines within an organisation for archiving, retaining, and destroying enterprise data. The policy should account for the personnel, processes and technologies required to ensure that enterprise data is archived and destroyed as needed, to meet business objectives and legal obligations

Disaster Recover Plan (DRP) / Business Continuity Plan (BCP)
A set of policies, tools, and procedures to enable the recovery and/or continuation of critical business components following a natural or human-induced disaster. A DRP will contain more specific information pertain to technology infrastructure and systems. These plans will contain details of the various personnel involved in the recovery process and their respective responsibilities.

Employee Awareness Training
Training programs which provide employees with anti-fraud training at least annually (including but not limited to detecting social engineering, phishing training, business e-mail compromise and other similar exposures).

Encryption
A method by which information is converted into secret code that hides the information's true meaning.

Endpoint Protection and Response (EDR)
Software installed on individual computers (endpoints) that is an integrated endpoint security solution which combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

Incident Response Plan
Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Information Asset Inventory
A list of all IT hardware and devices an entity owns, operates, or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Information Officer
The person responsible for encouraging responsible persons to comply with the principles and conditions for the lawful processing of personal information and assisting data subjects to make requests and lodge complaints.

Intrusion Detection/Prevention System
A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Managed Service Provider
A third party organisation that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Multi-Factor Authentication
A process in which a user authenticates themselves through two or more different means when gaining access to a computer system or web-based service. Typically use a password and a passcode, generated by a physical token device or software as the two factors.

Patch Management
Process of managing an IT network by regularly performing patch deployment to keep the network up to date. Each patch deployed is a set of changes to a computer program or its supporting data which is designed to update, fix or improve it to resolve vulnerabilities.

Payment Card Industry Data Security Standards (PCI DSS)
A set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

Penetration Tests
Authorised simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Privileged Access Management (PAM)
It is a combination of tools and technology used to secure, control, and monitor access to an organisation's critical information and resources. This process is done through limiting user access according to authority level and job function.

Sender Policy Framework (SPF)
An email authentication technique which is used to prevent spammers from sending messages on behalf of your domain.

Vulnerability Scan(s) / IT Audits
Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

WAP2 / WAP3 Encryption
A type of encryption used to secure the vast majority of Wi-Fi networks. It provides unique encryption keys for each wireless client that connects to it. WPA3 provides a more secure connection than WPA2.