Core Security Principles

Inventories

The organisation maintains inventories of Sensitive Data[1] and all assets that are used to process and/or store Sensitive Data[2].

Personnel

Only Authorised Persons[3] are permitted to access Sensitive Data.

Access Control

Secure MFA[4] is always applied on access points[5] to Sensitive Data.

Encryption

Sensitive Data are securely encrypted[6] in storage (‘at rest’) and transmission (‘in transit’).

Configuration and Patching

Assets that are used to process and/or store Sensitive Data are appropriately configured and patched.

Secure Cloud Storage

Sensitive Data are stored using secure cloud services.[7]

Backup

Sensitive Data are securely backed up[8] on a [daily][9] basis.

Devices

Physical devices that are used to access Sensitive Data are secured[10] and handled securely[11].

Kiowa
INFORMATION SECURITY

NOTES

1. ‘Sensitive Data’ means information that requires protection for legal, regulatory or contractual reasons, e.g., Personal data (PII), Intellectual Property (IP).

2. For example, physical devices (PCs, laptops) and resources such as cloud services

3. ‘Authorised Persons’ comply with some or all of the following: Pre-employment screening; formal authorisation by senior management; NDA; information security responsibilities in Terms of Employment; security awareness training.

4. Generally approved types of MFA such as those using authenticator apps or FIDO2

5. For example, logins to cloud services and VPNs

6. Approved algorithms and procedures, i.e., AES256 for storage, TLS1.2 or greater for communications security.

7. The implicit intention of this item is to say ‘we don’t store Sensitive Data on devices or relatively insecure resources such as emails’. Where possible, Sensitive Data are transmitted using secure cloud file sharing services.

8. Backups are securely encrypted and logically and physically segregated.

9. Backup frequency depends on business and regulatory/contractual requirements.

10. Secure devices are installed with appropriately configured and updated endpoint protection, and securely configured in terms of password security and automatic inactivity timeout.

11. Securely handled devices are used in consideration of the risk that they may be stolen, damaged or accessed by unauthorised persons.

Kiowa
INFORMATION SECURITY