Maitland

Information Security Protection Controls

Table of Contents

1. INTRODUCTION

1.1 The heart of digital crime is all about illegally obtaining or manipulating information – being one of the most valuable assets of Maitland and any other organisation. In order to effectively and efficiently protect our information assets in light of the changing threat landscape, (i.e. the vanishing perimeter, Advanced Evasive Techniques (AETs), Advanced Persistent Threats (AETs), and Malware-less / Anomalous behaviour) a shift in paradigm is required.

1.2 As a global organisation, Maitland relies on the confidence that its clients have in its business activities, which includes the protection of their sensitive data (Personal Identifiable Information, Contractual, Financial, Intellectual Property). In order to protect this data Maitland applies several strategies (layers of defence) that make it difficult for threat actors such as insiders / criminals / syndicates to perpetrate their crimes through the exploitation of our information assets and systems.

1.3 Maitland takes the issue of collecting and processing your personal information seriously. Maitland makes every effort to comply with the EU's General Data Protection Regulation (GDPR) which governs the collection and processing of personal identifiable data, in order to protect the confidentiality, integrity, availability and privacy of the data subject by ensuring that it is secure.

1.4 Other privacy laws such as the South African Protection or Personal Information (POPI) Act (POPIA) similarly requires the safeguarding of personal identifiable data to ensure it is kept secure against the risk of loss, unauthorised access, interference, modification, destruction and disclosure.

1.5 We continue to ensure that we are current with best practise frameworks (security and privacy) in order to meet client, security and regulatory control requirements.

2. GDPR PROGRAMME

2.1 Maitland complies to the EU General Data Protection Regulation (GDPR).

2.2 Maitland has an appointed Data Protection Officer (DPO) tasked to provide the necessary oversight function, strategy and implementation of GDPR within the organisation.

2.3 The Maitland Group, ICT and Information Security teams have implemented, and continue working diligently towards maturing, controls related to GDPR requirements.

2.4 Maitland Group Information Security function uses reasonable measures and continues to invest, improve, refine and implement such measures to safeguard sensitive and personally identifiable information.

3. PRIVACY AND INFORMATION SECURITY

3.1 ICT and Group Information Security at Maitland treat privacy and the security of personally identifiable information very seriously and the Maitland Group continues to invest in information security to ensure compliance with GDPR and other applicable privacy laws.

3.2 Information security in the Maitland Group is aligned to the Secure Controls Framework (SCF) (ISO 27001/2 is a subset of this control framework universe) which defines an Information Security Management System (ISMS) as an overarching framework to manage privacy and personal information as part of the broader management of information risks, information security and related compliance, incident management and business continuity issues.

3.3 Following a risk based approach, the measures that have been and continue to be selected are deemed appropriate to the type of information maintained, and always considers applicable laws regarding safeguarding any such information under our control, in particular personal and sensitive data.

3.4 Existing information security controls are maintained, and new controls have been designed and implemented to detect or prevent unauthorised access to, modification or destruction of personal information, whether accidental or deliberate. These controls are based on the requirements of the business and conform to commonly accepted industry standards as well as contractual and legal requirements.

4. INFORMATION SECURITY MANAGEMENT SYSTEM

4.1 An Information Security Management System that is in place, is based on SCF which is more holistic than the traditional ISO/IEC 27000 and NIST frameworks.

4.2 Information Security in the Maitland Group is embedded into the company through participation in various forums and structures and the Group Information Security Head provides regular reporting directly to the Board and the Audit and Risk Committee.

4.3 The Group Information Security policy is regularly reviewed and updated to ensure continued information security compliance to legal and regulatory requirements.

5. INFORMATION SECURITY AWARENESS TRAINING

5.1 Information Security awareness training is implemented and forms part of the Induction programme for all new joiners.

5.2 Information security and data protection training is compulsory for all staff.

6. DATA PROTECTION

6.1 Maitland recognises how important it is to protect the confidentiality, authenticity and/or integrity of information and adopts a defence-in-depth approach, i.e. no reliance is place on any one single security control.

6.2 Maitland uses Transport Layer Security (“TLS”) encryption technology and encrypts communications to enhance data privacy and help prevent loss, misuse, or alteration of the information under Maitland’s control. Maitland also implements encryption mechanisms for data at rest.

6.3 Security is managed with mechanisms to protect entry points to the network, the network is segregated to provide security and protect the confidentiality and availability of Maitland’s personal and sensitive information.

6.4 Security managed services are provided as a hybrid of in-house and outsourced with contractual and service level agreements are in place with suppliers for managed services.

7. DATA TRANSFER

Due to the global nature of the Maitland Group, appropriate steps are taken to manage the risks associated with cross border transfer and we continue to monitor legislative and regulatory requirements in meeting data flow requirements.

8. BUSINESS APPLICATIONS

8.1 Business applications that process personally identifiable and sensitive information have been identified at Maitland.

8.2 A gap analysis has been performed for each application to identify functionality to comply with GDPR requirements, to determine potential gaps in each application and to develop a remediation roadmap in fulfilling the GDPR compliance requirements.

9. AUDITS

9.1 Internal audits of ICT and Information Security are performed at Maitland by the internal audit department.

9.2 ISAE 3402 audits are performed for an independent assurance opinion on controls for financial reporting.

10. CYBER SECURITY INSURANCE

Maitland's Firm-wide insurance programme includes Cyber cover through the Professional Indemnity (PI) policy and the separate Cyber policy. The Cyber insurance cover in place reflects types of events Maitland insures against. For example, electronic wire fraud is a cyber event covered under the crime section of our PI policy.

11. HUMAN RESOURCE SECURITY

Maitland carries out background verification checks on relevant candidates for employment, includes information security responsibilities in agreements with employees and contractors and requires compliance with policies. A disciplinary process exists to take action against employees in the case of a data breach.

12. DATA CLASSIFICATION

12.1 Maitland has a data classification and handling policy to protect information related to its importance.

12.2 Maitland has various measures to detect and prevent unauthorised disclosure, modification, removal or destruction of information stored on media. Various solutions have been implemented on user end-point devices to manage, detect and as best possible prevent use of removable media for personal or sensitive data.

12.3 System policies are continually being refined to improve our capability in managing, detecting and preventing the use of removable media and e-mail for personal and sensitive information.

13. ACCEPTABLE USE OF ICT

13.1 The Acceptable Use policy governs acceptable use of information assets including mobile devices.

13.2 Maitland's ICT has put in place resources and continues to manage information assets responsibly and requires that employees and external party users to return all Maitland assets on termination of their employment, contract or agreement.

13.3 Maitland ICT continually reviews its management of assets and continues to identify information assets and maintaining an inventory of assets associated with Maitland's information.

14. USER ACCESS CONTROL TO SYSTEMS AND APPLICATIONS

14.1 User registration and de-registration follows a defined process and users of Maitland's information assets only receive access to the Maitland network and related services for which approval has been given.

14.2 User access reviews are performed periodically to ensure and to reduce the risk of unauthorized access to systems and services. User access is removed to systems and applications upon termination of their employment, contract or agreement.

14.3 The Acceptable Use policy makes users accountable for safeguarding their authentication information. The Acceptable Use policy is presented to users at log on requires acceptance before authenticating a user to Maitland's network.

14.4 To prevent unauthorised access to systems and applications, access to information and application system functions are restricted and log-on is secure on all relevant applications and systems, with multifactor authentication mechanisms, complex passwords that meet or exceed current standards.

14.5 User accounts that are not accessed / remain dormant within a period of 60 days will be automatically disabled. This will be applied on a continuous basis in order to reduce the attack surface area of malicious threat actors aiming to target accounts.

15. PHYSICAL AND ENVIRONMENTAL SECURITY

15.1 All Maitland's business data and the technology that process or stores data are hosted in secure data centres that are (ISO 9001, 27001, PC-DSS) compliant.

15.2 Physical protection measures, to safeguard against unauthorized physical access, damage and interference to the organization's information and information processing facilities, have been implemented.

15.3 Data centres have the necessary environmental controls, access control, back-up and uninterrupted power supplies, to reduce the possibility of loss, damage, theft, compromise and likelihood of an interruption to Maitland's operations.

16. OPERATIONS SECURITY

16.1 Information security operating procedures are continually developed, refined and reviewed to meet existing and new client, regulatory and best practise requirements. This is to ensure correct and secure operations of information processing facilities.

16.2 The Maitland Change Management policy governs changes, including security changes, to Maitland business processes, information processing facilities and systems, and requires that all changes follow the change management process.

16.3 Development, testing, and production environments are physically or logically separated, where it is required, to reduce the risks of unauthorised access or changes to the operational environment.

17. MALWARE AND VULNERABILITY MANAGEMENT

17.1 Maitland's information processing facilities are protected against malware and the implemented anti-malware and machine learning technologies detect, prevent, and can recover against known malware.

17.2 The Information Security Office have controls in place to prevent the exploitation of technical vulnerabilities, by managing technical vulnerabilities and performing regular vulnerability scans to identify technical vulnerabilities of information systems being used. Maitland's exposure to such vulnerabilities is evaluated and the appropriate measures are taken to address the associated risk. Penetration tests are conducted on a periodic basis to test the effectiveness of the vulnerability management process.

18. BUSINESS CONTINUITY AND DISASTER RECOVERY

18.1 Business continuity, disaster recovery and security continuity are part of Maitland's business continuity management system. The business continuity processes are documented, implemented and maintained.

18.2 IT disaster recovery is tested regularly to ensure availability of information processing facilities. The major information processing facilities (data centres) have appropriate standby recovery facilities (data centre).

19. INCIDENT MANAGEMENT

Maitland has an established incident management process and incidents are logged and tracked, which includes data breaches. The incident process is continually improved to allow for additional business, regulatory, or best practise requirements.

20. DATA RETENTION AND DESTRUCTION

20.1 Maitland has an approved Data Protection, Retention and Destruction policy, that sets out the policy with respect to Data Protection, Data and Document Retention, Archiving and Destruction and applies to all staff across Maitland.

20.2 ICT performs backups of Maitland's information hosted on the ICT managed infrastructure, software and systems. Backups are tested regularly to protect against loss of data and in accordance with Maitland backup processes.

20.3 Reviews are performed for each application to identify data aging capabilities and comply with the GDPR requirement to keep information only for as long as needed. A formal GDPR roadmap is monitored in this regard.

21. COMPLIANCE

Group Information Security continues to support the business by designing, implementing and managing solutions that promote and ensure compliance with legal and contractual requirements, to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

22. WORKING FROM HOME / WORKING REMOTELY

Staff working from home (WFH) / from remote locations comply to the Maitland Information Security and Acceptable Usage policy principles which highlight some key aspects as follows:

- Usage of the existing Maitland remote access control and authentication mechanisms with only approved Maitland end user compute devices;
- Avoidance of public WI-FI hotspots when connecting to the corporate network;
- Physically Securing your end user compute device and not leaving it unattended, i.e. applying secure practises within your home;
- Ensuring that end user compute devices are only used for the intended purposes granted by the organisation and not for personal or shared use;
- Ensuring that adequate safeguards, i.e. strong passwords, software updates/patches, are implemented on home WIFI networking equipment; and
- Ensuring that documents, sensitive business data and other work-related materials are kept confidential and secure in the home office location.

Maitland
January 2021