Baseline Security Standards

1. Introduction

1.1 This document defines a set of baseline generic information security controls applicable to any computerized information system within MTD. Additionally it provides guidance to administrators, developers and security personnel to assist in enhancing the security of implementation of applications and the technologies that underpin them.

1.2 Securing a system involves implementing a set of procedures, practices, and technologies to protect the information technology (IT) infrastructure as well as software and associated data throughout MTD.

2. Objectives

2.1 To define a set of baseline generic information security controls applicable to any computerised information system in MTD.

2.2 To provide guidance to administrators, developers and security personnel to assist in enhancing the security of implementations of applications and the technologies that underpin them.

3. Scope

3.1 Controls specified in this document apply to all IT platforms.

3.2 All of MTD's information systems will be subject to the policies specified within this generic security standard. The policies will be applied to new and existing installations.

3.3 This is a generic standard. Controls specific to particular technologies are not defined here but will be the subject of additional standards.

4. Installation and Configuration

4.1 Operating Systems

4.1.1 The latest version of the operating system should be installed wherever possible.

4.1.2 The most secure implementation of the operating system should be selected at installation time. All default unused services should be disabled during installation.

4.1.3 All available patches/updates for the operating system should be applied upon availability subject to testing by approved system owners.

4.1.4 All servers should be connected to an uninterruptible power supply by ensuring that server rooms are served with UPS capability.

4.2 User Configuration

4.2.1 User Administration

4.2.1.1 Each user must be given a unique account with which to access an information system.

4.2.1.2 Account login time restrictions should be put in place to prevent access outside of required working hours. Determine required access times for users and place them into time based access groups, this will minimize active accounts outside normal working hours.

4.2.1.3 All requests for user account creation must be duly authorised. The creation of a user account must be recommended by the immediate superior and approved by the Head of IT.

4.2.1.4 User accounts should be set up in accordance with the predefined naming convention.

4.2.2 Default Accounts

4.2.2.1 Guest accounts and all non-essential default accounts should be deleted / disabled from the system following initial installation. Wherever possible, generic accounts should be avoided.

4.2.2.2 If possible, the Administrator account should be renamed and a decoy Administrator account with no privileges should be created.

4.2.2.3 The passwords of all accounts created during software installation must be changed from their default values immediately upon completion of the installation.

4.2.3 Authentication/Password Configuration

4.2.3.1 Prior to logon, all systems must display a warning message advising of the consequences of misuse and that monitoring of usage may be performed.

4.2.3.2 The system should prevent password re-use for at least 5 changes. The password history function should be used for this purpose.

4.2.3.3 User account passwords must expire after a maximum of 60 days. A warning message should appear 15 days before a password is scheduled to expire.

4.2.3.4 Passwords must be at least 7 characters in length should contain at least one non-letter character (special character or number). This is set to meet the password complexity requirement.

4.2.3.5 The account lockout should be enforced after 5 unsuccessful attempts to login. The duration of lockout should be set to 30 minutes and automatically reset after 30 minutes.

4.2.3.6 The user must be forced to change the password when accounts have been newly created or after a password reset.

4.2.3.7 Workstations should allow the user to lock their workstation without the need to logout of the underlying applications.

4.2.3.8 Workstations should have an idle timeout facility such that after a period of Inactivity for 15 minutes, the user must re-authenticate to resume access. This is to ensure unauthorised access to the workstations.

4.2.4 Privileges and Access Control

4.2.4.1 Programs, utilities and application software should be developed to run with the minimum of privileges to successfully perform their function. Grant only those privileges specifically identified as required.

4.2.4.2 Non-administrative users must not be granted administrative privileges or rights.

4.2.4.3 User accounts should be created and maintained with the fewest privileges required to successfully execute the user's job function.

4.2.4.4 Processes and procedures should be developed to control access to the super user/administrator account. The password for this account should be maintained under management control. All system administration should be performed using named accounts owned by the individual administrators.

4.2.4.5 Access or functionality provided to users at remote or untrusted locations should be kept to a minimum level.

5. Auditing and Monitoring

5.1 Events to be Audited

5.1.1 The security events recorded within the log of an Information Asset must be sufficient to establish individual accountability for actions performed and be able to support the investigation and resolution of suspected violations.

5.1.2 Audit logs must be reviewed periodically to identify security incidents or suspicious pattern of events.

5.1.3 Audit log content must not be visible or modifiable to non-privileged users.

5.1.4 Audit log records must be retained for a minimum of 6 months.

6. Security Compliance

6.1 Security Management

6.1.1 When any staff leaves the organisation all access must be disabled effective from the last day of the service.

6.1.2 Four (4) weeks after a user leaves, with the approval of the Head of IT, all accounts that belong to the leaver must be deleted. At which time any files owned by these accounts must be either deleted or reallocated.

6.1.3 Systems Administrator must conduct an audit of their user community in order to ensure that each user has a continuingly valid need to access the information asset.

6.1.4 The addition, modification and deletion of users must create an appropriate audit trail, which identifies when change was done, by whom and the authorising party wherever applicable.

6.1.5 All systems must have a nominated IT Custodian.

6.1.6 Audit logs must be protected from deletion from non-privileged users.

6.2 Security Compliance Checking

6.2.1 The administrators must have and make use of security administration tools, which facilitate the identification of security weaknesses e.g. dead, unused or inappropriate accounts, accounts without password protection or accounts with weak passwords.

6.2.2 Live data must not be supplied to external organisations for the purpose of testing application changes or for the diagnosis/resolution of problems.