ISC10D025

Overview of Security Policy Revisions Drafted

Following the security breach in the Climatic Research Unit an independent audit of IT security was commissioned, among other things this audit recommend changes to a number of our IT security policies. A summary of the changes that have been made is included below and copies of the full policies are included on the following sections.

There is further work that has been recommended which we plan to complete for the June ISSC meeting:

- **Security Manual SM11.1 Information Classification and Data Policies** – as recommended by 7safe to generally review, make more applicable to research data and to link to record management policies
- **Security Manual SM10.1 Anti-Malware and Workstation Specific Controls** – as recommended by 7safe to review and 'beef' up as critical part of desktop security.

Summary of changes made

General Information Security Policy (GISP)

Changes for security review project and following recommendations from external security consultants (7Safe)

General

- Used 'Information Services' throughout rather than 'Information Services Directorate' or 'IT and Computing Service'.
- Used 'departments' throughout rather than 'School/Units'.
- References to 'Personnel' changed to 'Human Resources Division'.

GISP2 Conditions of Computer Use

- Changed 'Incident response' text to be consistent with 'Reporting Breaches' in the CoCU.

GISP4 Identification, authentication and authorisation

- 4.3 authorisers for access to data changed from 'data owners/administrators' to just 'data owners'.

GISP 5 Use of passwords

- 5.3 reference to SM5.2 'Password checking and enforcement ' removed and propose removal of the whole SM5.2 following 7Safe recommendations. SM5.2 was never implemented fully because of technical difficulties and having this policy necessitated copying of password hashes to another machine for checking and this in itself poses another security risk.
- Incident response also changed accordingly.

GISP24 Liability of students' own systems and content

- 24.2 changed ‘Residences Network Terms and Conditions’ to ‘Self-Registered Equipment Terms and Conditions’.

Security Manual

SM5.1 Password Assignment

- General changes for consistency e.g. changing ‘IT and Computing Service to ‘Information Services’.
- Under ‘Audit and accountability’ changed ‘SCI senior IT support staff’ to ‘SCI School IT Managers’.
- Under ‘Implementation’ SM5.1.1 added requirement for administrator passwords to be minimum of 15 characters.
- SM5.1.4 – changed wording to be technically more accurate as suggested by 7Safe
- SM5.1.5 – Inserted link to procedures for communicating passwords to users and also drafted this document .
- SM5.1.6 – Reference to password checking and enforcement removed.

SM5.2 Password Checking and Enforcement – REMOVED

SM5.3 System Administrator Passwords

Some fairly extensive changes

Server Administrators

- SM5.3.1 - Stresses using membership of an administrator rights group as the means of giving IT support staff administrator access to servers.
- SM5.3.2 - Some changes to wording.

Desktop local admin accounts

- SM5.3.6 - Stresses membership of AD administrator groups as means of giving admin access to IT support staff on user machines in their care.
- SM5.3.7 – Stresses need for separate admin groups for each dept.
- SM5.3.8 – Restricted access by IT support to local system administrator account passwords as per 7safe reccs.
- SM5.3.9 – Deals with users requiring admin rights on their machine
- SM5.3.10 – Disabling local admin accounts use in all but Safe Mode
- SM5.3.11 – Same password assignment rules as for servers
- SM5.3.12 - IT support access to local admin passwords
- SM5.3.13 – Local admin passwords changed when IT support staff who kew them leave
- SM5.3.14 – Storage/security of local administrators passwords