HP Records Manager

Security Model

1. Preamble

This document is issued in accordance with the Records Management Policy. It describes the features of the HPRM security model, which is based on the principle of access to information on a need to know basis. The document should be read in conjunction with the HPRM Business Rules at the following link for a comprehensive appreciation of the requirements and capabilities of HPRM.

2. Security Profiles

Within HPRM, employee positions are matched with the staff members holding those positions. Security permissions are then based on the roles and duties associated with each position. This enables the employee to access any sensitive information necessary to undertake the duties of that position. Should the incumbent change positions then that person would relinquish his/her current profile and inherit the security profile attached to the new position. Section Heads should advise the HPRM System Administrator if any position change impacts on an employee's requirement to access sensitive information within HPRM.

3. HPRM Security Model

There are three elements of security which collectively control access to sensitive information contained within HPRM. These are: security classifications, caveats and access control. Security classifications and caveats are applied to both people and records. Access Control is applied to records to limit access of sensitive records to particular group of people (usually business groups).

4. Security Classifications

The security classifications of 'Confidential' and 'Unclassified' are applied to distinguish sensitive information from other business material so that caveats and if appropriate, access controls can be applied to secure sensitive information.

'Unclassified'
This security classification is associated with documents and files that are open to all HPRM users. These documents should not contain 'confidential' or sensitive information. All University staff that use HPRM will have this minimum security associated with their account. Whilst these records may not be particularly sensitive they are not generally available in the public domain and accordingly are restricted for use within the University or by authorised contractors or consultants. This classification is used for records which document the majority of daily business, including deliberative and decision making processes.

‘Confidential’

This is the security classification applied to all files and documents which contain sensitive material of any kind. Examples include documents that contain commercial, legal, financial or personal details. This level of security will only be available to staff who occupy positions which require access to sensitive information.

5. Caveats

For additional control, confidential material needs to be categorised and allocated a caveat according to whether the subject matter relates to students, staff, legal matters etc. Appropriate Access Controls can then be applied to limit these records to relevant business groups. Caveats must therefore be used with the security level of ‘Confidential’ and always in conjunction with appropriate Access Controls.

A HPRM user who has ‘confidential’ access and the necessary caveats within his/her HPRM security profile and is in an appropriate Access Control group will be able to view and interface with those confidential documents and files necessary to undertake his/her duties.

Staff in Confidence

This caveat applies to documents which contain the personal or employment details of an individual. Typically, this would include records relating to salary, allowances, appeals, counselling, discipline and grievances. Committee records which relate to the appointment and promotion of staff would also be restricted by this caveat.

Student in Confidence

Student in Confidence applies to information relating to the personal, financial and academic progress details of an individual student. This also includes records relating to appeals and to academic and other misconduct.

Commercial in Confidence

This caveat relates to commercially sensitive information and may include records such as:

- Service Level Agreements
- Building and Maintenance Contracts
- Service and Non-Service Contracts
- Tender Documentation
- Deed of Assignments
- Consultancy Agreements
- Leasing Agreements

Complaints in Confidence

This caveat applies to documents relating to complaints made against the University and lodged by organisations, members of the public, staff and students. Complaints in Confidence also apply to complaints about staff and students.

Committee in Confidence

This caveat applies to minutes, agendas and correspondence relating to confidential committee business.

Security in Confidence

Security in Confidence is applied to sensitive records concerning the investigation and reporting of security incidents and to records relating to the security of university premises.

Legal in Confidence

This caveat applies to sensitive information concerning legal matters, for example records relating to litigation and legal advice from both internal and external sources.

Industrial in Confidence

This caveat is used for sensitive information pertaining to the formal relations with the University's employees and their representatives. Includes negotiations conducted to obtain determinations, agreements or awards, industrial disputes settled within the University or by an external arbiter and reports on the state of industrial relations within the University.

Honours and Awards

This caveat is used for sensitive records that pertain to the bestowing of honours and awards on University staff and students by Flinders University or other agencies or organisations.

6. Access Control

Access control is the next level of security in which identified sensitive information can be restricted. This additional file or document control is applied below the security and caveat level. This means that access control will not bypass core security permissions. Controls can be applied to give varying degrees of access to individuals and work groups, organisational units, committee or project members who have the right security profile.
The following access controls can be applied within HPRM:

- View Document - Gives 'read' only permission
- View Metadata – Gives permission to see record data but it is limited to defined properties and the document cannot be viewed
- Update Record – Gives permission to view and amend the document, the original version is retained and a new document will be added
- Update Records Metadata – Gives permission to modify record data, but is limited according to other defined properties i.e. User Type, Security etc
- Modify Record Access – Gives permission to add or remove users and edit access control properties for the file or document.
- Destroy Records – Gives permission to mark the records for destruction. This control will only be available to the System Administrator
- Contribute Contents – A User must have this permission to add contents to a file.

7. System Audit

The HPRM System Administrator will automatically receive reports of security breaches. Typically, this would occur when a document classified as confidential is saved to an unclassified file. All security breaches will be investigated. In the former example, the System Administrator/Manager University Records will determine whether or not the document was indeed confidential and requires further protection through the creation of an access control group.