



TRIM Security Guidelines

This document is an initiative of the Records Management Unit

INDEX

- Overview.....3
- Security Levels.....4
 - [No Security Level].....4
 - Public.....4
 - Unclassified.....4
 - Confidential.....4
- Caveats.....5
 - Staff in Confidence.....5
 - Commercial-in-Confidence.....5
 - Student-in-Confidence.....5
 - Complaints-in-Confidence.....6
 - Old System Files-Access Restricted.....6
 - Establishment-in-Confidence.....6
 - Industrial-in-Confidence.....7
 - Staff Complaints.....7
 - Staff Discipline.....7
 - Student Complaints.....8
 - Student Discipline.....8
- Access Controls.....8
 - Record Access Control Restriction Options.....9
 - Grouped Access Control Restriction Options.....9
 - Context Class Object Access Control Restriction Options.....9

Overview

The security framework set up for TRIM allows the application of Security Levels, Caveats and Access Controls, to comply with Records Security Guidelines, for appropriate access to electronic documents retained in TRIM.

Documents placed into TRIM are to be allocated appropriate Security Levels, Caveats and Access Controls according to the content which is contained in the document. Identified groups of documents that are deemed 'confidential' or 'sensitive,' or that contain personal information about an individual, must be protected from misuse, loss and unauthorised access, modification and disclosure.

University employees, who have access to TRIM, are to be allocated appropriate Security Levels, Caveats and Access Controls to access documents they require as part of their legitimate employment duties.

The University organisational structure is replicated in the 'Locations' table in TRIM. This is set up in hierarchical order, Business Unit – Section – Position – Employee/Staff Member, to facilitate appropriate access to documents. Positions in TRIM are allocated a security profile, against which an employee is placed. The security profile is based on the business activities undertaken for that particular position.

For example, if part of a 'Faculty Executive Officer' position's role deals with student enrolments, the position would be allocated a Security Level of 'Confidential' with the addition of a 'Student-in-Confidence' Caveat.

It is not considered appropriate that all positions that have a specified security level and caveat would necessarily require/have access to corresponding documents across the whole of the University. The use of Access Controls assists in restricting the access of documents to specified positions, groups, committees, business units and project teams where it is appropriate.

For example, if the "Faculty Executive Officer" position that deals with the student enrolment documents is located within the Faculty of Arts and the role includes interaction with Student Administration and the Conservatorium of Music, then it may be necessary to include all these business units to allow access to the documents concerned. This position would have no business reason to access any other enrolment documents from other faculties or schools, and to do so would fall outside the legitimate employment duties of the individual occupying that position.

In addition to this, the TRIM access controls have the additional flexibility to provide a tiered effect on what aspect of information is restricted through the use of 'view metadata', 'view document', 'update document', 'update document metadata', 'modify record access', 'destroy records', and 'contribute contents'.

For example, you may allow all staff that deal with documents that have a security level of Confidential and Complaints-in-Confidence to view the metadata of a document only, but not be able to view or edit the document. This enables the sharing of knowledge that a document exists, but provides a level of security that documents cannot be viewed without permission being sought from the originating business unit.

With the application of all three levels of security we are able to provide access to documents as deemed appropriate for the content contained and in the context of who needs access to the information as part of their legitimate employment duties..

The examples provided are a guide only and do not illustrate all the possible documents. If in doubt, seek advice.

Security Levels

Security Levels are the first level of Security which determines the accessibility of documents. These levels are:

[No Security Level]

Use this security level for all external Locations in the Locations/Contacts database in TRIM. It is not used for University of Tasmania documents or folders created in TRIM.

Public

Use this security level for folders and/or documents that are deemed open to public access and are not of a 'confidential' or 'sensitive' nature. For example, documents that are published on the internet public domain.

All University staff, that has access to TRIM, has access to this level of security.

Unclassified

Use this security level for folders and/or documents that are deemed open to all staff members of the University that do not contain 'confidential' or 'sensitive' information. For example, internal guidelines, procedures and protocols.

Positions that are allocated this level of security will be able to view all documents that are 'Unclassified', 'Public' or 'No Security Level'.

Confidential

Use this security level for folders and/or documents that contain information that is deemed 'confidential' or 'sensitive' in nature. Information that for commercial, legal, financial, safety or public relations reasons, should not be released or disclosed.

Only available to officers authorised by Head of Business Units.

Positions that are allocated this security level will be able to view all documents that are 'Confidential', 'Unclassified', 'Public' or 'No Security Level'.

Caveats

Security Caveats are the next level of security in which sensitive information can be restricted. If a caveat is applied it must be used with a security level of Confidential. Caveats can be used in conjunction with Access Controls.

Only positions that have been allocated a specific caveat can access documents with the same caveat applied.

Staff in Confidence

Use for anything relating to individual staff members. See Policy Document – No 4, Privacy Policy for definitions relating to ‘personal information’, ‘employee information’, ‘collection’ and ‘sensitive information’.

Refer to Staff Complaints-in-Confidence or Staff Discipline-in-Confidence caveats for security for staff complaints or discipline issues respectively.

It is mandatory that this be used in conjunction with an Access Control such as a Business Unit, specified positions or group.

Examples of documents that would require the application of this security caveat would include:

- Letters of Appointment.
- Allowances.
- Employment Conditions.
- Leave.
- Performance Management.
- Overtime/Salary.
- Separations.
- Honours/Awards.

Commercial-in-Confidence

Use for commercially related information such as agreements, contracts etc.

Use in conjunction with an Access Control such as a Business Unit, specified positions or group where appropriate.

Examples of documents that require the application of this security caveat may include:

- Service Level Agreements (external).
- Building & Maintenance contracts.
- Tender Documentation including Request for Tenders, Tender Committee Agendas, Minutes and associated documentation.
- Deed of Assignments.
- Consultancy Agreements.
- Leasing Agreements.

Student-in-Confidence

Use for information relating to individual students. See Policy Document – No 4, Privacy Policy for definitions relating to ‘personal information’, ‘sensitive information’, ‘collection’, and ‘counselling information’.

Refer to Student Complaints-in-Confidence or Student Discipline-in-Confidence caveats for security for student complaints and discipline issues respectively.

It is mandatory that this caveat be used in conjunction with an Access Control such as a Business Unit, specified positions or group

Examples of documents that would require the application of this security caveat would include:

- Enrolment forms.
- Update of personal details.
- Applications for financial assistance.
- Examination details.
- Results.
- Variations of enrolment.

Complaints-in-Confidence

Use for formal complaints directed at the University of Tasmania and lodged by the public, University employees or students. Excludes complaints relating to individual staff or students (refer to Student Complaints or Staff Complaints in relation to complaints directed at individuals).

To be used in conjunction with an Access Control such as a Business Unit, specified positions or group as appropriate.

Examples of documents that would require the application of this caveat would include:

- Complaints relating to access to buildings.
- Complaints relating to conditions of accommodation.
- Complaints about campus locations.
- Complaints about excess travel.
- Complaints about course quality.
- Complaints about Information Technology (IT) such as network speed and accessibility.

Old System Files-Access Restricted

This caveat is used to restrict access to legacy folders which were uploaded into TRIM. Security was based on controlling the physical access to paper format records contained in subject classified folders.

Access is based on the business needs of the position.

Establishment-in-Confidence

Use for sensitive issues relating to the establishment and changing of University structure through establishing and reviewing positions, classification and grading of positions and preparation of organisational charts.

To be used in conjunction with an Access Control such as a Business Unit, specified positions or group as appropriate.

Examples of documents that would require the application of this security caveat would include:

- Position Descriptions
- Reclassification of Positions
- Draft Organisational Charts
- Committee minutes and agendas that relate to the reorganisation of the structure of the University

Industrial-in-Confidence

Use for sensitive information pertaining to the establishment of formal relations with the University's employees and their representatives to achieve a harmonious workplace. 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.

To be used in conjunction with an Access Control such as a Business Unit, specified positions or group as appropriate.

Examples of documents that would require the application of this security caveat would include:

- Negotiations for Awards and Agreements relating to pay and working conditions.
- Industrial action including lockouts, strikes, bans, stop work meetings.
- Records documenting determinations and decisions of the Industrial Commission.
- Committee Minutes, Agendas and associated documents relating to any of the above and disputes.

Staff Complaints

Use for informal and formal complaints relating to individual staff members. Refer to Harassment & Discrimination Policy and refer to specific Staff and Academic Agreement. Refer to Staff Discipline-in-Confidence caveats for security caveat to be applied to records for disciplinary action that may be brought against a staff member.

It is mandatory that this caveat be used in conjunction with an Access Control such as a Business Unit, specified positions or group.

Examples of documents that would require the application of this security caveat would include:

- Allegations of harassment/discrimination.
- Allegations of defamation.
- Agendas, Minutes and associated documents of committees.
- Outcomes to complaint.

Staff Discipline

Use for informal and formal discipline cases relating to individual staff members. Refer to Harassment & Discrimination Policy and Staff and Academic Agreement. Use the Staff Complaints caveat for security for matters relating to complaints made against staff.

It is mandatory that this caveat be used in conjunction with an Access Control such as a Business Unit, specified positions or group.

Examples of documents that would require the application of this security caveat would include:

- Appeals on decisions regarding discipline case.
- Committee Minutes, Agendas and associated documents relating to disciplinary case.
- Notification of decisions regarding discipline case.

Student Complaints

Use for informal and formal complaints relating to individual students. Refer to Ordinance 8 Student Complaints, and the Harassment and Discrimination Policy. Refer to Student Discipline for disciplinary action that may be brought against a student.

It is mandatory that this caveat be used in conjunction with an Access Control such as a Business Unit, specified positions or group.

Examples of documents that would require the application of this caveat would include:

- Complaints regarding results of assignments/examinations.
- Complaints regarding perceived acts of discrimination/harassment against a student.
- Complaints about academic exclusions.
- Committee minutes or agendas relating to a complaint
- Appeals against outcomes of complaint decisions.

Student Discipline

Use for informal and formal discipline cases relating to individual students. Refer to Ordinance Student Discipline 9, and the Harassment and Discrimination Policy.

It is mandatory that this caveat be used in conjunction with an Access Control such as a Business Unit, specified positions or group.

Examples of documents that would require the application of this caveat would include:

- Allegations of general or academic misconduct.
- Disciplinary proceedings relating to discrimination/harassment allegations against a student.
- Appeals against decisions relating to academic or general misconduct.
- Committee minutes or agendas relating to a student discipline matter.
- Notification of outcomes of decisions.

Access Controls

Access controls are the next level of security in which sensitive information can be restricted.

Access control applies to many types of objects and operates using the following rules.

Record Access Control Restriction Options

Access Control is an additional object control that is applied below security level and caveat security. This means that access control will not bypass core security (Security levels, caveats and user type permissions).

Access control is an individual security control and is applied to individual records:

- Access control can be applied to many records using the tag function. This means that all tagged records will be given the same access properties (where allowed – existing “modified access” permissions).

Each access control property may be set individually, however all properties work collectively. This determines that all properties have a default value (unless determined elsewhere the default access will be public).

Access control restriction options for records are:

- View Document – Gives read only permission to the group for the electronic attachment (if it exists).
- View Metadata – Gives permission to the group to see record data, but it is limited according to other defined properties (User Type, Core Security etc).
- Update Document – Gives full permission to the group for the electronic attachment (if it exists).
- Update Record Metadata – Gives permission to the group to modify record data, but is limited according to other defined properties (User Type, Core Security, etc)
- Modify Record Access (Group members, and access properties) – Gives permission to the user to add or remove group members and/or edit the access control properties for the record.
- Destroy record – Gives permission to the group to mark the record for destruction.
- Contribute Contents – the rule is that a user must have this permission to add contents to the container (folder/box), regardless of the ‘Update Record Metadata’ access control setting on the container (folder/box).

Grouped Access Control Restriction Options

All objects that can have access controls applied to them allow the following group methods of applying the controls. The group properties can be applied to access controls are:

- Public – allows everyone access
- Container – (for records only) – the record adopts the Access Controls applied to a container (folder) record. This option uses cascading container relationships.
- Private – Is an exclusive setting allowing only the property editor access
- Custom – allows the editor to define group members for the property using either adding individual positions, business units, project teams, committee members etc..

Context Class Object Access Control Restriction Options

TRIM Context modules such as workflow, record types, reports etc constitute class objects. These objects must have scalable access control properties that determine

access to the module and/or the impact of access on child objects such as locations, records, workflow etc.

The ability to use or modify entries in these modules is dependent of the following access controls:

- Can Use – allow users to view and therefore use the item
- Can Update – allow users to modify the item
- Can Modify Access – allow users to modify who may change the access controls for the item.
- Can Delete – allow users to delete the item.