# Information Classification and Handling Guidelines

## 1. Purpose

Southern Cross University routinely gathers, stores, processes, transmits and disposes of information. That information must be readily available to those who need it. However, it must also be protected from unauthorised disclosure, misuse and misrepresentation.

These Guidelines outline the University's standard data classifications and the standard handling controls required to protect University information. They support the University's legal obligation to ensure that private information is managed in accordance with the principles outlined in the *Privacy and Personal Information Protection Act 1998* (NSW), the *Health Records and Information Privacy Act 2002* (NSW), the *State Records Act 1998* (NSW), and the University's Privacy Management Plan. The provisions of these documents must be taken into account while applying these minimum standards.

## 2. Information Classification

Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to the University's operations.

- **Confidentiality** of information refers to limiting access to information to authorised persons for approved purposes.
- **Integrity** of information refers to the assurance that information is authentic, correct and valid, and can be trusted.
- **Availability** of information refers to allowing authorised persons to access information for authorised purposes at the time they need to do so

The University uses the following information classification:

| Classification | Business Impact Level | Type of information |
|---|---|---|
| **Public** | No business impact.<br>Compromise of information would be expected to cause no damage to the University or others. | Information that is publicly available such as:<br>• Staff directory information<br>• Course information<br>• Published research data |
| **Private** | Low business impact.<br>Compromise of information would be expected to cause no (or insignificant) damage to the University or individuals | Most routine information such as work unit processes and procedures |

| Classification | Business Impact Level | Type of information |
|---|---|---|
| **Sensitive** | Medium business impact.<br><br>Compromise of information would be expected to cause damage to the University or individuals. | Includes the following information:<br><br>• Personal information of staff, students or others<br>• Information subject to legal privilege<br>• Commercial-in-confidence information |
| **Highly sensitive** | High business impact.<br><br>Compromise of information would be expected to cause significant damage to the University or individuals. | Includes the following information:<br><br>• Health information of staff, students or others.<br>• Personal information of staff, students or others that is information about:<br>  ○ racial or ethnic origin<br>  ○ political opinions<br>  ○ membership of a political association<br>  ○ religious beliefs or affiliations<br>  ○ philosophical beliefs<br>  ○ membership of a professional or trade association<br>  ○ membership of a trade union<br>  ○ sexual orientation or practices<br>  ○ criminal record<br>• Highly confidential information. |

The University's sensitive and highly sensitive classifications align with the following NSW government DLM labels:

- OFFICIAL: Sensitive – Legal
- OFFICIAL: Sensitive – Health Information
- OFFICIAL: Sensitive – Personal
- OFFICIAL: Sensitive – NSW Government

## 3. Information Handling Guidelines

Handling means the way in which information is managed, how the information is accessed, stored, transferred or transmitted, shared, archived and disposed of. Sensitive information is important as it could contain personal or health information

and if compromised, could cause limited damage to the University or individuals. As a result, a higher level of controls to protect and manage this information is required.

The University's handling requirements are based on the NSW government's minimum handling requirements for sensitive and highly sensitive information.

| **Collecting** |
| --- |
| Collect information only for a lawful purpose that is reasonably necessary, and directly related to a function or activity of the University. Collection methods, including online surveys, must have secure storage. |
| Label digital information that is collected. This includes information captured via automated processes, for example via batch processes or API. This information should be labelled in metadata if the system allows or via system documentation ideally at the time the system is developed. |
| **Labelling** |
| Label highly sensitive information at the time of collection or creation. Labelling is not retrospective. If information is not in use, there is no need to re-label with new labels. Information in use should be re-labelled. |
| If receiving information that is already labelled, do not re-label. If there are questions about the validity of the label consult the data originator. |
| Labelling of entire systems and large datasets needs to be carefully considered as this could restrict access to information unnecessarily. Labelling at field, case or record level may be more appropriate if the system has the capability. Access to field, case or records with higher sensitivity within a system or large dataset can be managed via user access permissions, only giving access to users that need-to-know. |
| **Monitoring** |
| Monitor information over time to determine if the sensitivity of the information has changed. Change the label and security classification if required. |
| Keep access audit logs for the appropriate retention period to assist in future audit and access control monitoring. Protect these logs from accidental or deliberate modification. |
| **Storing** |
| Store hard-copy records and information in a designated location, in lockable storage or secure access areas.<br>Store digital records, information and data in the University's recordkeeping systems or business systems. |
| Maintain inactive sensitive data to reduce risk of loss or theft. The risk of exposure of sensitive data increases when applications are retired or migrated, or SharePoint sites and file shares are abandoned at the conclusion of a project. For specific guidance about migration or retiring applications, check with Technology Services. |

| Accessing |
| --- |
| Apply the need-to-know principle to all information classified as sensitive or highly sensitive. |
| Access to information classified as sensitive and highly sensitive should be restricted. The information custodian has overall accountability for access provided (to hard copy, digital records, information and data). |
| Ensure access to information classified as sensitive or highly sensitive is only provided for a clear and legitimate business reason. |
| Manage user access on an ongoing basis as roles and personnel change. The need for ongoing access or a time limited period of access should be considered. |
| Review access to information systems containing information classified as sensitive or highly sensitive by directly linked third party applications. Information made available to these third party applications must be limited to need-to-know. User access of the third party applications need to be controlled as does the level of information that the users of this application can view. |
| Access rights cannot be transferred. Usernames and passwords should be kept confidential and not shared. |
| **Securing** |
| University officers must assess all data transiting and at rest and make an assessment whether it should be encrypted. |
| Protect assets which contain sensitive or highly sensitive information such as laptops or mobile devices. |
| Secure mobile devices after use in a lockable room within University facilities and if possible, outside of University facilities, for example if working from home. |
| Do not use your device unless it is safe to do so. Be aware of your surroundings. When information is being used that can be read, viewed, heard or comprehended, it may be at a higher risk of compromise. Different physical environments pose different risks for information compromise. |
| **Using** |
| Lock your computer screen or log out of secure systems when you leave your desk and make sure hard copies are secure (clear desk and clear screen policies should be implemented). |
| Train all staff using sensitive or highly sensitive information or using a secure system, so they are aware of the nature of the sensitive or highly sensitive information and the rules which apply to use the information. Rules include whether they can view, print, share, or email information. |

| |
|---|
| Manual transfer of information classified as highly sensitive may be passed by hand within a discrete office environment provided it is transferred directly between members of staff who need-to-know and there is no opportunity for any unauthorised person to view the information. |
| When carrying physical information classified as sensitive outside a University facility, this information is to be carried in an opaque envelope or folder. |
| Do not access information classified as sensitive using public networks. |
| Do not copy information classified as sensitive onto local drives or removable mobile storage devices such as USBs. |
| ***Using – Reports, Dashboards and Products*** |
| Do not display products such as reports or dashboards containing sensitive or highly sensitive information unless the audience need- to-know, and permission has been sought from the data custodian. |
| **Sharing** |
| If sharing data externally, reducing the sensitivity of the information by de-identification techniques is recommended, for example removing personal information or information revealing law enforcement procedure. |
| If sharing information externally, it is preferable that the source information is redacted to conceal the sensitive or highly sensitive information where possible. This ensures that the source information remains inviolate and that the information can be safely shared. Care must be taken that the redaction does not alter the source information. |
| Emailing highly sensitive information should be done via secure file transfer protocol, or via a secure system as recommended by the University. Highly sensitive information should not be stored in emails or as attachments to email in your inbox.<br>Email systems are at higher risk of compromise than approved University business systems and are at risk of accidental forwarding. |
| Sensitive and highly sensitive information should only be shared for authorised purposes. |
| **Archiving, Retention and Disposal** |
| Records, information and data are covered by the requirements of the State Records Act 1998. Sensitive and highly sensitive information must be disposed of securely. Guidance should be obtained from Corporate Records. |