# **Access Classification Labels and Access Permissions**

# 

# Background

From mid-2024, digital records transferred to QSA will be visible to their controlling agencies via ArchivesGateway. Because this access includes not only the metadata of the digital records but also the ability to download the record itself (or a digital copy of a physical record), the system has been set up to provide agencies with a means to control user access.

Access to digital records in ArchivesGateway will follow the principle of least privilege, ensuring that users will only have access to what they absolutely need in order to perform their responsibilities. This will help your agency to protect the information within your records and prevent unauthorised access to digital records.

Access Classification Labels have been implemented as a mechanism to ensure that sensitive information is only accessible to users with the approved and allocated permissions.

## What is the principle of least privilege and why is it important?

The principle of least privilege (PoLP) is a security concept that emphasizes limiting the access rights of individuals, processes, or systems to the minimum level necessary for them to perform their tasks. This principle is crucial in the context of a trusted repository, where sensitive and valuable data or assets are stored. The principle of least privilege:

1. **Mitigates Risk and Minimises Exposure:** By adhering to the principle of least privilege, the risk of unauthorised access, data breaches, or malicious activities within the repository is minimised.
2. **Protects Sensitive Information:** Our trusted repository will store sensitive and confidential information. Applying the principle of least privilege ensures that only individuals with a legitimate need for access can retrieve and access specific records. This helps safeguard sensitive information and maintains the confidentiality and integrity of the stored data.
3. **Ensures Accountability:** Limiting access rights enhances accountability by clearly defining who has access to the repository and what actions they can perform. In the event of security incidents or unauthorised activities, it becomes easier to trace and identify relevant users.
4. **Adapts to Changing Requirements:** The principle of least privilege facilitates adaptability to changing business requirements or security policies. As roles and responsibilities evolve, access permissions can be adjusted accordingly. This ensures that individuals only have the access they need for their current responsibilities, minimising the chance of outdated or unnecessary permissions lingering in the system.

In summary, the principle of least privilege is a fundamental security measure in trusted repositories, helping to protect sensitive data, mitigate risks, and maintain a secure and controlled environment.

## Access Classification Labels and definitions

Records (both physical and digital) in ArchivesGateway will be classified as non-sensitive, sensitive, or highly sensitive.  The classification will be applied to the transfer list by the agency, in consultation with QSA, at the point of Transfer.

***Non-sensitive*** - Use for records where there is little risk to the relevant person or agency if the information is released. Examples of non-sensitive records can include photographs of open events, routine correspondence and records of hearings heard in open court. Any Agency user in ArchivesGateway can view non-sensitive digital or digitised records that are controlled by their agency, regardless of permission levels.

***Sensitive*** - Use for records which contain sensitive information about a person, event or business activity that poses medium or moderate risk to the person or agency if it is released before the restricted access period has expired. This may include information subject to legal professional privilege, personal information, or information about law enforcement operations. Only Agency users with the ‘Access Sensitive’ permission can access Sensitive records in ArchivesGateway.

***Highly sensitive*** - Use for records which contain detailed information of a sensitive nature about a person, event or business activity that poses a high risk to the person or agency if it is released before the restricted access period has expired. This may include sensitive medical records, culturally sensitive material, confidential financial records, or security related information. Only Agency users with the ‘Access Highly Sensitive’ permission can access Highly Sensitive records and they can only be accessed through the File Issue service.

Please note that these values differ to the [Queensland Government Information Security Classification Framework (QGISCF)](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-classification-framework-qgiscf), and this will have to be considered as agencies set the value for this field.

## Access Permissions in ArchivesGateway and Access Classification Labels

Permissions within ArchivesGateway are set up using a three-tier hierarchy based on the sensitivity of the records. This ensures that access to records and metadata is only granted to users with the approved and allocated permissions in accordance with the Access Classification Labels that have been applied. For further information on the three permission types in ArchivesGateway and what levels of access they cover, please refer to the table below:

|  |  |  |
| --- | --- | --- |
| Permission Level | How it’s displayed in ArchivesGateway | Coverage |
| Generic Access | *No Permissions set* | The most basic setting for generic users does not include any permissions and only grants visibility to records and metadata that are either classified as non-sensitive or do not have an Access Classification assigned. ArchivesGateway users at this level can see the metadata of Sensitive records but not the records themselves. They can see the metadata of Highly Sensitive records only if it is also published to be visible to the public in ArchivesSearch. |
| Access Sensitive | *allow\_access\_sensitive* | This permission level allows users to see the metadata of all records that have an Access Classification of Sensitive, Non-sensitive, or that don’t have an Access Classification assigned. They will also be able to see digital records with these Access Classifications. If users have File Issue permissions, they will be able to request these records through the file issue service. |
| Access Highly Sensitive | *allow\_request\_highly\_sensitive* | This permission levels allows users to see all records. This includes records that have an Access Classification of Highly Sensitive, Sensitive, Non-sensitive, or with no Access Classification assigned. While users will be unable to see Highly Sensitive digital records in ArchivesGateway, they will be able to request them through the file issue service. They will also be able to request digital and physical representations with an Access Classification of “Highly Sensitive.” |

### Summary of ArchivesGateway Access Permissions/ Access Classification Labels

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **No Permissions set** | **allow\_access\_sensitive** | **allow\_request\_highly\_sensitive** |
| **Non- Sensitive Records** | **Metadata** | √ | √ | √ |
| **Download Digital copy** | √ | √ | √ |
| **Sensitive Records** | **Metadata** | √ | √ | √ |
| **Download Digital copy** | X | √ | √ |
| **Highly Sensitive Records** | **Metadata** | o | o | √ |
| **Download Digital copy** | x | x | √  (Via File Issue Request only) |

o - only if published to ArchivesSearch. Please note that in these instances, only the metadata is published to ArchivesSearch, however the link to the digital object is not.

## Security Administrators in ArchivesGateway

All Access Classification permissions in ArchivesGateway are managed by the Security Administrators via the ***allow\_security\_administration\_*permission.** This is the highest permission level, allocated to a recommended maximum of two users from an agency at any given time. The granting of this permission is determined by an agency’s Chief Executive Officer and is applied by QSA to Senior Agency Administrator users in the system. Security Administrators automatically inherit all Access Classification permissions.

If you would like any further information or advice, please contact us via email [digitalarchive@archives.qld.gov.au](mailto:digitalarchive@archives.qld.gov.au). We are here to help!