Appropriate Access to Data and Information

When transmitting data and information that are classified as Protected A, B, or C, special safeguards will be needed.

The sample access safeguards are only intended to outline possible solutions; as such, **they are not prescriptive** and do not elaborate on the particulars (i.e., the complete context in which the data and information exists) or the manner in which security classification is applied (i.e., to a system and application, record, or specific field).

Sample Access Safeguards

Classification	Access Restrictions	Audit/Activity
Public	• Can be made open to the public and all employees, sub-contractors and agents. • Can be published, but does not have to if it is of no value/interest to the public. Determination to publish material is made by business area.	• None.
Protected A	• Authorized access (employees, contractors, subcontractors and agents) on a "need-to-know" basis for business related purposes.	• Periodic audits to show that protection is, in fact, occurring.
Protected B	• Limited to individuals in a specific function, group or role.	• Pre-clearance based on position or contractor, subcontractor or agent relationship. • Log of access/actions. • Periodic audits of adequate protection.
Protected C	• Limited to named individuals (positions).	• All access or actions will be logged and subject to non-repudiation processes as appropriate.

For more information, please refer to Safeguarding Government Information or contact your Sector Information Security Officer (SISO).