Transmitting Data and Information

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

The sample transmission 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 Transmission Safeguards

Classification	Print/Hard Media	Digital Files
Public	• No special safeguards.	• No special safeguards.
Protected A	• Sealed envelope. • First class mail.	• Message sent in such a way to prevent interception, modification, or unauthorized receipt en route or at destination. • When personal information is included in a digital file, appropriate security measures, based on the sensitivity of the data and/or information, must be in place.
Protected B	• Sealed envelope stamped confidential. • Receipt confirmation required.	• Message sent in such a way to prevent interception, modification, or unauthorized receipt en route or at destination. • When personal information is included in a digital file, appropriate security measures, based on the sensitivity of the data and/or information, must be in place. • Receipt confirmation required. • Audit of access points is suggested.
Protected C	• Tamper evident packaging (e.g., double-sealed envelope with inside envelope signed to reveal evidence of tampering). • Transmitted under a continuous chain of custody with receipts covering each individual who obtains custody.	• Message sent in such a way to prevent interception, modification, or unauthorized receipt en route or at destination (e.g., encryption used to send/authenticate message). • Complete audit trail at each access point.

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

Alberta