Directive on Security Management - Appendix J: Standard on Security Categorization

Note to reader

The Standard on Security Categorization took effect on July 1, 2019. It replaced parts of the Security Organization and Administration Standard that was in effect from June 1, 1995 to June 30, 2019).

Appendix J. Standard on Security Categorization

J.1 Effective date

J.1.1 This standard takes effect on July 1, 2019.

J.2 Standards

J.2.1 This standard provides details on the requirements set out in subsection 4.3.1.

The procedures and subsections are as follows:

Procedure	Subsection
The security categorization process	J.2.2
General security categories	J.2.3
Information confidentiality categories	J.2.4

J.2.2 **The security categorization process** is as follows:

J.2.2.1 Examine separately the potential for injury that results from a loss of confidentiality, integrity or availability.

J.2.2.2 Assign security categories as follows:

J.2.2.2.1 A single security category that indicates the overall impact of a compromise (see subsection J.2.3); or

J.2.2.2.2 Separate security categories that indicate potential impacts of losses of confidentiality, integrity and availability (see subsection J.2.4), as applicable.

J.2.2.3 Apply the following considerations, as appropriate, when assigning a security category:

J.2.2.3.1 Confidentiality pertains mainly to information but can also pertain to assets;

J.2.2.3.2 The security category of services pertains mainly to their availability but can also pertain to their integrity; and

J.2.2.3.3 Assigning a security category for information and assets must also consider the following:

a. Overall monetary and non-monetary value; and
b. The impact that could result from unauthorized destruction, theft or removal;

J.2.2.4 The security category for information or asset repositories reflects the impact of aggregation, where more significant injury may occur when a group of information resources or assets is compromised;

J.2.2.5 The security category determines, in part, security requirements and, consequently, needs to balance the risk of injury against the cost of applying safeguards throughout the life cycle of information, assets, facilities or services; and

J.2.2.6 From a confidentiality standpoint, the security category for information considers the exemption and exclusion criteria of the Access to Information Act and the Privacy Act to ensure that resources are not applied to protect information that can be made public.

J.2.3 **General security categories** (impact levels) are as follows:

J.2.3.1 Information, assets and services are categorized as “very high,” “high,” “medium” or “low” impact to reflect the degree of injury that could reasonably be expected as a result of a loss of confidentiality (resulting from unauthorized disclosure), loss of integrity (resulting from unauthorized modification or destruction), or loss of availability (resulting from unauthorized removal or other disruption):

J.2.3.1.1 **Very high:** Applies when a compromise could reasonably be expected to cause severe to exceptionally grave injury;

J.2.3.1.2 **High:** Applies when a compromise could reasonably be expected to cause serious to severe injury;

J.2.3.1.3 **Medium:** Applies when a compromise could reasonably be expected to cause moderate to serious injury; and

J.2.3.1.4 **Low:** Applies when a compromise could reasonably be expected to cause limited to moderate injury.

J.2.3.2 Information, assets and services are considered non-sensitive if no injury would result from their compromise. For the purpose of assigning a

security category, such information, assets and services can be assigned an impact level of “low.”

J.2.4 **Information confidentiality categories** are as follows:

J.2.4.1 **Classified:** Information is categorized as “classified” (that is, “Confidential,” “Secret” or “Top Secret”) when unauthorized disclosure could reasonably be expected to cause injury to the national interest:

J.2.4.1.1 **Top Secret:** Applies to the very limited amount of information when unauthorized disclosure could reasonably be expected to cause exceptionally grave injury to the national interest;

J.2.4.1.2 **Secret:** Applies to information when unauthorized disclosure could reasonably be expected to cause serious injury to the national interest; and

J.2.4.1.3 **Confidential:** Applies when unauthorized disclosure could reasonably be expected to cause limited or moderate injury to the national interest;

J.2.4.2 **Protected:** Information is categorized as “Protected A,” “Protected B” or “Protected C”

when unauthorized disclosure could reasonably be expected to cause injury outside of the national interest:

J.2.4.2.1 **Protected C:** Applies to the very limited amount of information when unauthorized disclosure could reasonably be expected to cause extremely grave injury outside the national interest, for example, loss of life;

J.2.4.2.2 **Protected B:** Applies to information when unauthorized disclosure could reasonably be expected to cause serious injury outside the national interest, for example, loss of reputation or competitive advantage; and

J.2.4.2.3 **Protected A:** Applies to information when unauthorized disclosure could reasonably be expected to cause limited or moderate injury outside the national interest, for example, disclosure of an exact salary figure.

ISBN:

Date modified:

2019-07-01