Link 5.5 Example Data Security Classification Framework

Three example frameworks are presented in the following tables.

Classification	Framework 1
Classification 1 (highest)	**Top secret:** Internal data that would adversely affect an organization's plans if the data were disclosed externally. Examples include plans to merge with another organization. This classification requires the highest level of security to prevent the data being released to external sources.
Classification 2	**Highly confidential:** Critical internal data that would impede the organization's operation if disclosed externally or to unauthorized sources internally. Examples include financial information and medical records. This classification requires high security with authorization given prior to copying or removing the data from the organization's premises.
Classification 3	**Proprietary:** Internal information relating to the operational procedures and product designs that should only be available to authorized internal and external sources. This requires high security with limited access given to internal staff and trusted external partners (following the completion of a nondisclosure agreement).
Classification 4	**Internal use:** Internal information generated and used within the conduct of normal business operations where disclosure may adversely affect the credibility of the organization. Examples include meeting minutes and emails. This classification requires normal security where staff are not expected to disclose information to external parties unless as part of agreed working practice.
Classification 5 (lowest)	**Public information:** Information which is available externally, such as annual financial reports. This classification requires minimal security to ensure data are only released through authorized channels with prior approval.

Classification	Framework 2
Classification 1 (highest)	**Business critical**: Information that if disclosed to unauthorized parties may put the organization at significant risk. Examples include financial accounts. This classification requires the highest level of security.
Classification 2	**Content sensitive:** Information that if disclosed to unauthorized parties may significantly affect the organization. This includes: ○ Commercially sensitive data, such as new product designs. ○ Personal sensitive data, such as financial and medical details. ○ Security sensitive data, such as passwords and transport schedules. This classification requires high security.
Classification 3	**Confidential:** Information that if disclosed to unauthorized parties may adversely affect the organization. Examples include daily cash flow reports. This requires high security.
Classification 4	**Internal use**: Information that may only be accessed by employees. Examples include purchase orders and delivery schedules. This classification requires reasonable security controls.
Classification 5 (lowest)	**Unclassified:** Information to which access may be granted to anyone. Examples include product descriptions. This classification requires controls to prevent unauthorized changes or deletion of the data.

Classification	Framework 3
Classification 1 (highest)	**Restricted:** Internal data that would place the organization at high risk if disclosed to unauthorized parties. Examples include new product developments. This classification requires the highest level of security.
Classification 2	Not in use.
Classification 3	Not in use.
Classification 4	**Private:** Internal data that would place the organization at moderate risk if disclosed to unauthorized parties. Examples include product stock levels. This is the default classification if no classification is specified and requires reasonable security controls to be adopted.
Classification 5 (lowest)	**Public:** Internal data that would place the organization at no or low risk if data were disclosed to unauthorized parties. Examples include the organization's history. This classification requires controls to prevent unauthorized changes or deletion of the data.