Data Classification Policy

Nexelus

Purpose

This policy will assist employees and other third-parties with understanding Nexelus' information labeling and handling guidelines. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect sensitive or confidential information (e.g., company confidential information should not be left unattended in conference rooms).

Scope

This policy applies to all information owned, managed, controlled, or maintained by Nexelus Information covered in this policy includes, but is not limited to, information that is received, stored, processed, or transmitted via any means. This includes electronic, hardcopy, and any other form of information regardless of the media on which it resides.

Roles and Responsibilities

The following teams have been developed and trained to define, maintain and monitor Asset Management Policy.

- HR & Finance is responsible for classification of all Human Resource data maintained and documented as per policy. The team members also include site leads at each Nexelus work site. The team leader is the Head of HR who reports to the CEO or the partner.
- Head of Engineering/Technology and Dev Team are responsible for classification of client data. The team leader is the Head of Engineering/Technology.

Definitions

- **Confidential/Restricted Data.** Generalized terms that typically represent data classified as *Sensitive or Private*, according to the data classification scheme defined in this policy.
- **Internal Data**. All data owned or licensed by Nexelus.
- **Public Information.** Any information that is available within the public domain.

Data Classification Scheme

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to Nexelus should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls

are appropriate for safeguarding that data. All data should be classified into one of the three following classifications.

Confidential/Restricted Data

Data should be classified as Restricted or Confidential when the unauthorized disclosure, alteration, or destruction of that data could cause a serious or significant level of risk to Nexelus or its customers. Examples of sensitive data include data protected by state or federal privacy regulations (e.g., PHI & PII) and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted and Confidential Data:

- Disclosure or access to Restricted and Confidential data is limited to specific use by individuals with a legitimate need-to-know. Explicit authorization by the Security Officer and/or the partner is required for access to because of legal, contractual, privacy, or other constraints.
- Must be protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure.
- Must be destroyed when no longer needed. Destruction must be in accordance with Company policies and procedures.
- Will require specific methodologies, procedures, and reporting requirements for the response and handling of incidents.

Internal Use Data

Data should be classified as Internal Use when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to Nexelus or its customers. This includes proprietary, ethical, or privacy considerations. Data must be protected from unauthorized access, modification, transmission, storage or other use. This applies even though there may not be a civil statute requiring this protection. Internal Use Data is restricted to personnel who have a legitimate reason to access it. By default, all data that is not explicitly classified as Restricted/Confidential or Public data should be treated as Internal Use data. A reasonable level of security controls should be applied to Internal Use Data.

Public Data

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to Nexelus and its customers. It is further defined as information with no existing local, national, or international legal restrictions on access or usage. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized alteration or destruction of Public Data.

Assessing Classification Level and Labeling

The goal of information security, as stated in the Information Security Policy, is to protect the confidentiality, integrity, and availability of Corporate and Customer Data. Data classification reflects the level of impact to Nexelus if confidentiality, integrity, or availability is compromised.

If a classification is not inherently obvious, consider each security objective using the following table as a guide. All data will be assigned one of the following four sensitivity levels.

CLASSIFICATION LEVELS

CLASSIFICATION	POTENTIAL IMPACT OF LOSS
RESTRICTED • Highly sensitive information • Level of protection is dictated externally by legal and/or contractual requirements. • Must be limited to only authorized employees, contractors, and business partners with a specific business need	**SERIOUS DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to Nexelus. Impact could include negatively affecting Nexelus' competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL • Sensitive information • Level of protection is dictated internally by Nexelus. • Must be limited to only authorized employees, contractors, and business partners with a specific business need	**SIGNIFICANT DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to Nexelus. Impact could include negatively affecting Nexelus' competitive position, damaging the company's reputation, violating contractual requirements, and exposing geographic location of individuals.
INTERNAL USE • Non-sensitive Information • Originating within or owned by Nexelus or entrusted to it by others. • May be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the public, due to the negative impact it might have on the company's business interests	**MODERATE DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to Nexelus. Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC • Information that has been approved for release to the general public	**NO DAMAGE** would occur if public information were to become available to parties either internal or external to Nexelus. Impact would not be damaging or a risk to business operations.

CLASSIFICATION	POTENTIAL IMPACT OF LOSS
• Freely shareable both internally and externally	

HANDLING CONTROLS PER DATA CLASSIFICATION

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	Required prior to access by non-Nexelus employees	Recommended prior to access by non-Nexelus employees	Not Required	Not Required
Labeling				
Internal Network Transmission (wired & wireless)	• Encryption Required • Instant Messaging Prohibited • FTP Prohibited	• Encryption Recommended • Instant Messaging Prohibited • FTP Prohibited	• No Requirements	• No Requirements
Labeling	?			
External Network Transmission (wired & wireless)	• Encryption Required • Instant Messaging Prohibited • FTP Prohibited • Remote Access if Necessary (only with VPN and two-factor authorization when possible)	• Encryption Required • Instant Messaging Prohibited • FTP Prohibited	• Encryption Recommended • Instant Messaging Prohibited • FTP Prohibited	• No special requirements
Labeling				

Handling Controls	Restricted	Confidential	Internal Use	Public
Data at Rest (file servers, databases, archives, etc.)	• Encryption Required • Logical Access Controls Required (Limit Unauthorized Use) • Physical Access Restricted to Specific Individuals	• Encryption Recommended • Logical Access Controls Required (Limit Unauthorized Use) • Physical Access Restricted to Specific groups	• Encryption Recommended • Logical Access Controls Required (Limit Unauthorized Use) • Physical Access Restricted to Specific groups	• Logical Access Controls Required (Limit Unauthorized Use) • Physical Access Restricted to Specific groups
Labeling				
Mobile Devices (iPhone, iPad, USB Drive, etc.)	• Encryption Required • Remote Wipe Enablement Required, if possible	• Encryption Required • Remote Wipe Enablement Required, if possible	• Encryption Recommended • Remote Wipe Enablement Recommended, if possible	• No Requirements
Labeling				
Email (with and without attachments)	• Encryption Required • Do Not Forward	• Encryption Recommended • Do not Forward	• Encryption Recommended • Do Not Forward	• No Requirements
Labeling				
Physical Mail	• Mark "Open by Addressee Only" • Use Courier or "Certified Mail" and	• Mark "Open by Addressee Only" • Use "Certified Mail" and Sealed,	• Mail with Company Interoffice Mail • US Mail or Other Public	• No Requirements

Handling Controls	Restricted	Confidential	Internal Use	Public
	Sealed, Tamper-Resistant Envelopes for External Mailings	Tamper-Resistant Envelopes for External Mailings	Delivery Systems	
Labeling				