SECURE CYBER GATES

DATA CLASSIFICATION POLICY

SECURE CYBER GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/DCP/020/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/RXT/037/1.0			Risk Exception Template

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective

The objective of this policy is to assist **Data Owners** in the evaluation of information (data) to determine, what level of security is required to protect data for which they are responsible.

Data Classification and Safeguard Standard:

- Outlines a data classification scheme used to define an appropriate level of protection
- Describes the overall process for classifying data and applying appropriate security controls
- Lists the security controls required based on the determined level of classification

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Accountable - Overseeing the implementation and enforcement of this policy [Review and Approve Policy]
DPO [Data Privacy Officer]	Responsible for creating ,updating, and maintaining this policy.
IT/Security Team	1. Responsible for ensuring Data classification protection requirements are in place 2. Responsible for enforcing these Data classification requirements
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy]
Employees / Contractors	1. Read this this Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

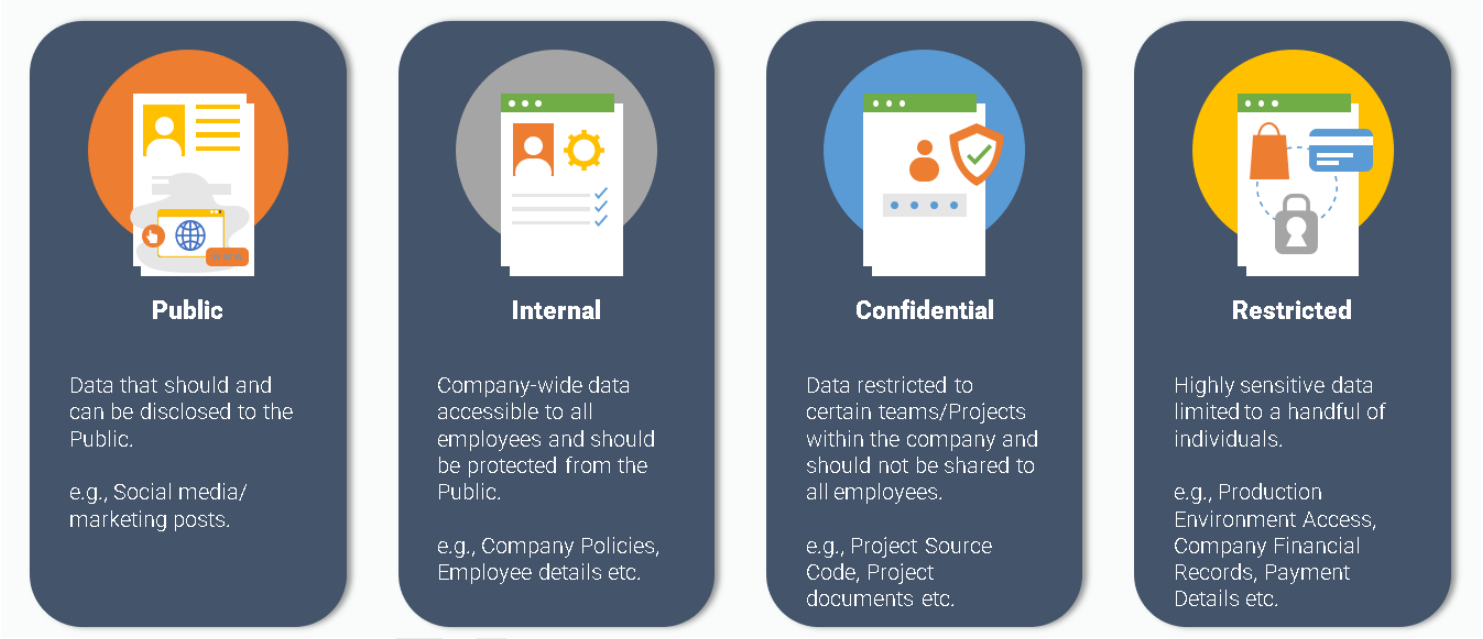
All **Employees/Contractors/Vendors** who come into contact with sensitive [SecureCyberGates] information are expected to familiarize themselves with this **data classification policy** and to consistently use these same ideas in their daily [SecureCyberGates] business activities. As stated in the introduction, both the data owners and data end users play a role in protecting [SecureCyberGates] information assets, and as such, they should become familiar with the data classification definitions and follow appropriate steps to ensure adequate data protection. All [SecureCyberGates] information assets should be accounted for and have a data owner whose role and responsibilities are clearly defined. Clearly defined accountability for all assets helps to ensure that appropriate levels of protection are identified, implemented, and consistently maintained. It is the responsibility of each [SecureCyberGates] data owner to classify his or her data

appropriately to ensure adequate protection. Security controls implementation may be delegated, but the accountability remains with the data owner.

4) Data Classification Description

A data classification framework will define sensitivity levels for data, categorizing it into **4 different classes** such as:

- Public
- Internal Use Only [Company-Wide use]
- Confidential
- Highly Confidential [Restricted]



4.1) Public Data

Access Controls

- Public data may be accessible to all General Public as well as all employees.
- Access should be controlled through authentication but can be less restrictive.

Encryption

- Encryption in transit is recommended for data integrity.

4.2) Internal Use Only Data

Access Controls

- Internal use data is limited to authorized employees. [All Company Employees]
- Access controls should ensure that only approved personnel can access this data.

Encryption

Encryption in transit is recommended for internal use data to prevent unauthorized interception.

4.3) Confidential Data

Access Controls

- Confidential data should have strict access controls, limited to individuals with a need-to-know.
- Accessible **ONLY to Some Employees** [e.g. Employee Working in Project A / Department A Should have access to only Data/Resources of Project A [And NOT any other Projects until required]
- Access must be carefully monitored and audited.
- MFA should be enabled for confidential data.

Encryption

- Confidential data should be encrypted both in transit and at rest to protect it from unauthorized access.

4.4) Highly Confidential Data/ Restricted

Access Controls

- Access to highly confidential data should be **tightly restricted and monitored.**
- **ONLY Few Employees have access**[e.g. Production Environment , Company Financial Records]
- Only personnel with specific authorization should have access.
- MFA should be enabled for highly confidential data.

Encryption

- Highly confidential data must be encrypted in transit and at rest with the strongest encryption protocols and key management.
- Transparent Data Encryption or Tokenization is required for column level encryption.

5) Data Labelling

Data owner shall label the data as follows:

- Public data do not require any labels
- All Electronic/Digital Documents MUST contain "Security Classification" Row under Document Control Page that should state **Public , Internal , Confidential , Restricted**
- All markings shall be displayed or stamped in the upper portion of each unbound page containing sensitive data. Data defined as Restricted, confidential, internal requires security labelling such as 'Restricted' or 'Confidential' or 'Internal use Only'
- Computer printouts and electronic materials shall have security labels in the footer
- Electronic media (disks, tapes, etc.) shall be clearly marked with the label
- Security Labels shall be in the front and outside back cover of printed materials
- Each data asset will have an assigned data owner responsible for determining its classification. Data assets will be labeled with their assigned classification levels, making it easy for users to identify and handle data according to its sensitivity.

6) Periodic Asset Recertification and Reclassification

The infrastructure, Security and legal compliance teams **periodically verify the asset inventory** to document latest updates, process for recertification's or upgrades or renewal of subscriptions where necessary. This procedure ensures validity of both physical assets & intellectual property over time. If asset characteristics change, including data sensitivity or hardware criticality, reclassification will be conducted. Reclassification will reflect the asset's current status.

7) Data Handling Guidelines

- Access control policies and procedures will align with data classification, ensuring that only authorized individuals can access sensitive data.
- Data classification will guide encryption requirements, with highly confidential data requiring strong encryption in transit and at rest.

8) Employee Training and Awareness

8.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

8.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

9) Compliance and Monitoring

9.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

9.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems , Application and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

9.3) Periodic Audits and Assessments : [SecureCyberGates]'s IT department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this security policy.

10) Escalation Matrix

10.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

10.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

10.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

11) Policy Exceptions

11.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

12) Policy Review and Updates

12.1) This policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

12.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

12.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

12.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for familiarizing themselves with the latest version of the policy and adhering to its requirements.

13) Conclusion

By implementing and adhering to this comprehensive Incident Management policy, [SecureCyberGates]aims to resolve incident ASAP and protect its sensitive information, intellectual property, and critical systems from unauthorized access and data breaches. This policy aligns with industry best practices and incorporates robust requirements for password construction, protection, management, and system development standards.

SECURE CYBER GATES

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://www.youtube.com/@SecureCyberGates
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES