# MEDIA SANITIZATION AND DISPOSAL POLICY

# DOCUMENT CONTROL PAGE

| | |
|---|---|
| **Document ID** | SCG/MSADP/022/1.0 |
| **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

This standard operating procedure (SOP) describes the procedure [SecureCyberGates] will use to sanitize and dispose of media containing information in a secure manner when no longer required, using formal procedures. **Data classification and Data retention Policies are already defined , please refer to document IDs SCG/DCP/020/1.0 AND SCG/DRTP/021/1.0**

# 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 / Retention and disposal protection requirements are in place<br>2. Responsible for enforcing these Data classification / Retention and disposal 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<br>2. Ask questions /Provide Feedbacks<br>3. Report possible or actual violations of this Policy. |

# 3) Scope

The policy contained herein applies to any person who has access to [SecureCyberGates]'s data and/or uses any of the [SecureCyberGates]'s Information resources/ assets. The purpose of this document is to elicit the best practices for data disposal associated with [SecureCyberGates] and sets the framework required to ensure data is disposed/destroyed in secure manner. This policy applies to both Tangible[Physical Assets like Papers Documents , USB , DVDs etc.] and Intangible media [Digital Assets like Documents , Database records , Software Licenses [Source Code] etc.].

# 4) Data Destruction Methods

| Name | Description |
|---|---|
| Secure Sanitization | The process of securely removing or overwriting data to prevent its recovery. For digital data, secure erasure methods in compliance with **NIST SP 800-88 standards** will be used to ensure that data is permanently removed from storage devices. [SecureCyberGates] will ensure that any cloud environment chosen for customer data is **NIST SP 800-88 compliant.** |
| Physical Destruction | The secure destruction of media to a level where data recovery is not feasible. For physical media, such as hard drives, optical discs, and paper documents, physical destruction methods including shredding, degaussing, or incineration may be used as appropriate. |
| Reuse of Hardware | The reallocation of hardware that may have contained sensitive information. |

# 5) Procedures

[SecureCyberGates] Leadership [Higher Management] in conjunction with the Legal team, Security Team, IT Team and Asset Owner:

(1) Uses industry-recognized secure practices to implement retention practices for data containing PII, based on [SecureCyberGates] 's documentation retention standards.

(2) Sanitizes or disposes of media containing Information when it is no longer necessary for business purposes through secure overwriting or physical destruction methods to ensure data cannot be reconstructed.

(3) The method of sanitization or destruction for media follows one of the following methods, based on the type of media:

**a. Physical Paper-Based Media:**

i. Internally or outsources the shredding process to a trusted third-party specializing in document destruction.

ii. Shreds non-sensitive paper-based media for recycling and securely shreds sensitive paper-based media.

**b. Physical Digital Media:**

i. Sanitizes digital media containing sensitive information through secure overwriting or physical destruction methods to render data recovery technically infeasible.

ii. Utilizes trusted third-party vendors for sanitization or destruction processes.

iii. Removes hard disk drives (HDDs) from systems before disposal.

iv. Tracks HDDs by serial number to ensure secure destruction.

v. Retains records of media sanitization or destruction in accordance with retention schedules.

(4) Reviews the media sanitization and disposal process annually or as required to address any non-conforming instances and adapt to evolving conditions, distributing

copies of updates to key personnel and communicating changes accordingly.

(5) Requests corrective action as necessary to address identified deficiencies, validates corrective action effectiveness, documents results, and requests additional corrective action if deficiencies remain unresolved.

# 6) Secure Destruction Facilities

If a third party is required to conduct destruction, only authorized facilities or vendors with a proven track record of secure data disposal may be selected. [SecureCyberGates] will maintain a list of authorized data destruction providers. [SecureCyberGates] will document the movement of data from its origin to the destruction facility and its final disposal to maintain a chain of custody Logs will be maintained for all data destruction activities, including the type of data, the method used, the date of destruction, and the personnel responsible for audit and compliance purposes. Upon data destruction, [SecureCyberGates] will obtain certificates of destruction from authorized facilities or vendors if such a certificate is available. These certificates will serve as evidence of proper data disposal. **Shredding machine is available at Common Area beside printing machine at Level 15A.**

# 7) Employee Training and Awareness

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

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

# 8) Compliance and Monitoring

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

8.2) 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].

8.3) 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.

# 9) Escalation Matrix

9.1) 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] |

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

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

# 10) Policy Exceptions

10.1) 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]]**

# 11) Policy Review and Updates

11.1) 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.

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

11.3) 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.

11.4) 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.

## 12) Conclusion

By implementing and adhering to this policy, [SecureCyberGates] aims to securely dispose media 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