Spurious Corporation

Information Technology Division
Policies & Procedures

Policy Issuance: Media Protection Policy and Procedures

Policy Issuance #800-53-MP

Responsible Department: Information Technology Division

Origination Date: 12/25/2015

Effective Date: 12/25/2015

CONTENTS

I. Policy Statement

This policy establishes, authorizes, and defines the Spurious Corporation Media Protection Policy and Procedures for the Company. This policy includes any Information Technology requirements and compliance with our federal partner's requirements as well as best practices for Company information technology security.

The Company's information systems capture, process, and store information using a wide variety of media. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media require special disposition to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality.

II. Purpose of Policy

This document establishes a policy for managing risks from media access, storage, transport, and protection through the establishment of an effective media protection program. The media protection program helps Company implement security best practices regarding enterprise media usage, storage, and disposal.

III. Policy Scope

This policy applies to all Company staff, volunteers, contractors, and persons providing services to a contract who access Company information and information systems which support the operation and data associated to the Company's System and Information Integrity.

This policy applies to all Company information systems, processes, and data. It also includes IT activities, and IT assets owned, leased, controlled, or used by the Company, Company' agents, contractors, and other business partners on behalf of Company.

All Company information assets must meet the required media protection controls defined in this policy document that are based on the *National Institute of Standards and Technology (NIST) SP 800-53 Security and Privacy Controls for Information Systems and Organizations*, and *Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns*. This document addresses the requirements set forth by the Company to implement the family of Media Protections controls. This policy provides requirements for the media

protection process to assure that information systems are designed and configured using controls sufficient to safeguard the Company's information systems.

The Company has adopted the Media Protection principles established in NIST SP 800-53, "Media Protection" control guidelines as the official policy for this security domain. The following subsections in this document outline the Media Protection requirements that the Company must implement and maintain to be compliant with this policy.

Where applicable, this policy includes protection of data that is Personal Identifiable Information (PII) or Federal Tax Information (FTI) within these security planning guidelines.

This policy shall be reviewed annually at a minimum.

IV. Definitions

A. **NIST:** The National Institute of Standards and Technology is a physical sciences laboratory and non-regulatory Company of the United States Department of Commerce. Its mission is to promote American innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

B. **Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies:** Provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Tax Information.

C. **FIPS 140 Security Requirements for Cryptographic Modules:** NIST issues the 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government.

D. **NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization:** The publication is a U.S. government document that provides clear methods of how to delete data from electronic media in a secure and permanent way. By following the guidelines, organizations can feel confident they have taken the necessary steps to minimize the chances of their data being recovered by third parties.

E. **Advanced Encryption Standard (AES) 256:** AES is a symmetric block cipher that the U.S. government selects to protect classified data. AES-256 encryption uses the 256-bit key length to encrypt and decrypt a block of messages.

F. **Restricted & Highly Restricted Data:** Numbers, characters, images, or other forms of output that are classified and/or protected by federal or state law, regulation, including FTI, PII, and/or other data in which access to defined information is restricted to defined stakeholders.

G. **Malware:** (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals, or conducts virtually any behavior an attacker wants. As malware comes in so many variants, there are numerous methods to infect computer systems.

V. Policy & Procedures

Note: The "MP" designator identified in each control represents the NIST-specified identifier for the Media Protection control family.

A. MP-2: Media Access

1. Media includes both digital media (diskettes and magnetic tapes) and external or removable hard drives. It also includes mobile devices including portable storage media such as USB thumb drives, portable computing, and communications devices with storage capability like notebook/laptop computers, tablets, smartphones and cellular telephones digital cameras, and audio recording devices. Non-digital media like paper and microfilm is also covered by this policy.

2. The Company requires that access to all digital and non-digital media is restricted to authorized individuals only using the Company's security measures, roles, and policies.

    a. Security controls are put in place to protect the confidentiality and integrity of data contained on all media from unauthorized disclosure and modification throughout the life of those storage media including disposal.

        i. This includes access controls such as physical protection, role-based security, firewall boundary protection, and encryption standards based on data classification.

B. MP-3: Media Marking

1. All data classifications must be reviewed at a minimum every year or when there is a significant change that may impact the security posture of the data or the system or both requiring a re-evaluation.

a. A significant change includes but is not limited to data aggregation/commingling or decoupling of data.

b. A re-evaluation may also occur when a system classified as low or medium risk is later interconnected with a system classified as high risk.

2. The Company must document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

C. MP-5: Media Transport

1. Restricted Data cannot be transmitted via fax.

2. Restricted Data cannot be transmitted via email.

a. An exception to this method of data transport applies if the email, contents, and attachments, are encrypted and delivered as a secured transmission by approved methods.

b. The data exchange process is reviewed and approved by the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

3. End-user devices including laptops or other removable storage media are prohibited from being used to transport Restricted Data.

D. MP-6: Media Sanitization

1. Before disposal or re-use, media must be sanitized in accordance with the *National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, Guidelines for Media Sanitization.* These methods ensure data is not unintentionally disclosed to unauthorized users.

2. Media containing Highly Restricted Data shall be sanitized prior to disposal, release out of Company control, or release for reuse by using Company approved sanitization techniques in accordance with applicable federal and Company standards and policies.

3. The Company protects data confidentiality and integrity through proper disposal of obsolete equipment and information by using secure software disposal techniques and/or destruction of the media.

a. The Company has disposal of records for receipt.

E. MP-7: Data Exchange Media and Methods

1. Media and methods used for transferring Restricted Data must be approved by both stakeholders involved in the data exchange.

    a. Technologies and brands may change over time but should include technologies such as Secure File Transfer Protocol (SFTP), Point-to-Point encryption, software solutions, related and approved resources to ensure protection of the data being exchanged.

2. Use of removable media is generally prohibited by the Company for the transmission of any Restricted Data.

3. Unless otherwise authorized, use of removable media for transferring FTI data can only be used if the data is encrypted on the device using the FIPS-140 encryption standard and only if the device is appropriately labeled and only if used for the purpose of off-site back-up storage in a secure safe within a secure building.

4. All media must be encrypted using FIPS 140-2 approved encryption algorithms like AES 256 unless the Company CIO or designee has classified the data as public.

    a. This includes but is not limited to devices such as USB thumb drives, external or removable hard drives, compact disks, magnetic tapes, etc.

5. All removable devices must be isolated and scanned for malware prior to use on the Company network.

    a. Autorun capabilities will be deactivated on all Company computers to reduce any risk of malware or other malicious attacks.

        i. Any detected malware must be removed from the media.

    b. The media must then be verified to ensure that it is safe for use on the Company network.

6. Data to be transferred will be prepared for electronic data exchange by the CISO or a designated and approved member of the Information Technology Infrastructure staff.

    a. This includes but is not limited to addressing file naming conventions, data and file encryption, format, and file type.

7. Data will be transferred using Company and stakeholder approved resources, software, media, and methods.

8. Designated IT staff performing data transfer activities must be approved by the CIO and/or CISO for this role.

9. Designated IT staff will work with the CISO to obtain any technical training necessary for performing secure data transfer functions.

10. Data exchange transactions will be documented to identify dates, sending Company, receiving Company, general description of documents or data being transferred, names of Company individual(s) involved in each transaction, and category of information.

    a. Logs will be maintained in a restricted access shared drive and will be available for review by the Company Information Assurance Office or authorized stakeholder representatives.

    b. See the Appendix for a sample log.

VI. Compliance

The Chief Information Officer, Chief Information Security Officer, and immediate Manager will be advised of breaches of this policy and will be responsible for appropriate remedial action as specified in the Confidentiality and Security sections in the *Spurious Code of Conduct Policy*.

VII. Roles and Responsibility

A. Chief Information Officer

1. Overall responsibility for the confidentiality, integrity, and availability of data and information;
2. Responsibility for implementing this policy within the Company;
3. May delegate the execution and maintenance of information technology security to the CISO.

B. Chief Information Security Officer

1. Facilitate Company IT Information Security ensuring that necessary safeguards are in place and working to meet Federal and other stakeholder requirements;
2. Coordinate digital information security activities throughout the Company.

C. IT Infrastructure Staff

1. Designated IT staff are authorized to participate in secure data transfer functions and tasks with CIO approval;
2. Designated IT staff members are responsible for monitoring, tracking, processing, and reporting secure data transfer activity;

3. All IT staff must report any breaches of this policy to the CIO and CISO.

VIII. References

Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns

National Institute of Standards and Technology SP 800-53 Security and Privacy Controls for Information Systems and Organizations

FIPS 140-3 Security Requirements for Cryptographic Modules

National Institute for Standards and Technology Special Publication 800-88 revision 1, Guidelines for Media Sanitization.

Spurious Corporation Code of Conduct Policy

IX. Revision History

Date	Version	Responsible	Reason for Revision
25 Dec 2015	1.0	IAO	Initial Draft
5 Jan 2021	1.1	IAO	Reformat and Updates
25 July 2022	1.11	IAO	Updated to use Company acronym
31 May 2013	1.2	IAO	Update for Company Policy Committee review

X. Appendices, Forms or Related Material

A. SAMPLE TRANSACTION LOG

Date	Sending/Receiving Company	Description	Company Staff Name(s)	Category (TOPs, FUTA, SUTA, etc.)

XI. Adoptions

This policy is hereby adopted on this ____ day of _____, 2023.

_____
Spurious Chief Information Officer

_____
Spurious Chief Executive Officer