**Spurious Corporation**

**Information Technology Division**
**Policies & Procedures**

**Policy Issuance: System and Communications Protection Policy and Procedures**

**Policy Issuance #800-53-SC**

**Responsible Department: Information Technology Division**

**Origination Date:12/16/2020**

**Effective Date: 1/11/2021**

## CONTENTS

I. Policy Statement
II. Purpose of Policy
III. Policy Scope
IV. Definitions
V. Policy & Procedures
VI. Compliance
VII. Roles & Responsibility
VIII. References
IX. Revision History
X. Appendices, Forms, and Related Materials
XI. Adoption

## I. Policy Statement

This policy establishes, authorizes, and defines System and Communications Protection controls for the Spurious Corporation. This policy includes any Information Technology requirements and compliance with our federal partner's requirements as well as best practices for Spurious Information Technology (IT) security.

The systems and communications protection policy establishes the rules necessary to properly establish network segmentation and boundary protection thought the organization as well as establishing the necessary rules around how cryptography will be implemented. Additionally, this policy establishes rules around allowed communication methods and mechanisms to ensure that the authenticity of those methods is maintained.

## II. Purpose of Policy

The purpose of this policy is to facilitate compliance with applicable federal and state laws and regulations, protect the confidentiality and integrity of Spurious' IT resources, and enable informed decisions regarding System and Communications Protection controls. It establishes the framework for System and Communications Protection for all Spurious information systems. Spurious Information Security Policies are the foundation for IT security for the Company. In addition, the purpose of this policy is to ensure controls are established to protect the confidentiality, integrity and availability of information and information systems by assuring systems, system components and services acquired are secure and do not negatively impact security of pre-existing systems used for conducting the Company's mission critical business functions. This includes, but is not limited to, data classification and management, communications, and encryption technologies.

## III. Policy Scope

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

This policy applies to all Spurious information systems, processes, and data; including IT activities and IT assets owned, leased, controlled, or used by Spurious, Spurious' agents, contractors, and other business partners on behalf of Spurious.

All Spurious information assets must meet the required security controls defined in this policy 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 Spurious to implement the family of System and Communications Protection controls. This policy provides requirements for the System and Communications Protection process to assure that information systems are designed and configured using controls sufficient to safeguard the Spurious information systems.

Spurious has adopted the System and Communications Protection principles established in NIST SP 800-53, "System and Communications Protection" control guidelines as the official policy for this security domain. The following subsections in this document outline the System and Communications 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 must be reviewed annually at a minimum.

## IV. Definitions

A. **NIST:** The National Institute of Standards and Technology (NIST) 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 FTI.

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. **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.

E. **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.

F. **Data at Rest:** refers to stored data and excludes data that is moving across a network or is temporarily in computer memory waiting to be read or updated. Data at rest can be archival or reference files that are rarely or never changed. It can also be data that is subject to regular but not constant change.

G. **Non-Privileged Account:** a standard user account that does not have elevated privileges such as administrator access to a system. For instance, non-privileged accounts cannot make configuration changes to an information system or change the security posture of a system.

H. **Privileged Account:** a system administrator account. Privileged accounts have elevated permissions than those of a non-privileged user account. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router management.

I. **Denial of Service (DoS) attack:** an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the service or resource they expected.

J. **Distributed Denial of Service (DDoS) attack:** a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic utilizing multiple compromised computer systems as sources of attack traffic.

## V. Policy & Procedures

**Note:** The “SC” designator identified in each control represents the NIST specified identifier for the System and Communications Protection control family.

### A. SC-2: Separation of System and User Functionality

1. Spurious must separate user functionality (including user interface services) from information system management functionality in application components.

2. For the application and database secure zones, an Company approved firewall or other network segmentation mechanism, for example micro segmentation or Virtual Local Area Networks (VLANs), is required to segregate application servers and database servers.

3. Information systems must prevent the presentation of information system management related functionality at an interface for non-privileged users.

4. Spurious internal network infrastructures (i.e., Company Local Area Networks [LANs]) must be segregated into network zones to protect application servers from the user LAN.

5. Production and non-production environments (e.g., test, development, QA, etc.) must be segregated from one another.

6. Wireless networks must be physically or logically segregated from internal networks such that an unknown external user cannot access a Company's internal network FTI, PII or National Directory of New Hires (NDNH) data.

7. Where technically configurable, Spurious must separate virtual machines with Highly Restricted Data from those with Unrestricted Data.

### B. SC-4: Information in Shared System Resources

1. Information systems must prevent unauthorized and unintended information transfer via shared system resources.

2. Information, including encrypted representations of information, produced by the actions of prior users and roles or the actions of processes acting on behalf of prior users and roles must not be made available for object reuse or shall residual information be made available to any current users or roles or current processes that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

3. Information systems must prevent unauthorized information transfer via shared resources in accordance with statewide information security standards when system processing explicitly switches between different information classification levels or security categories.

## C. SC-5: Denial of Service Protection

1. Spurious must limit the effects of DoS and DDoS attacks by appropriately securing all hosts that could be a potential target for a DoS or DDoS attack by doing the following:

    a. Denying all inbound traffic by default thus limiting the channels of network attacks.

    b. Periodically scanning network and devices for bots (software robots) and Trojan Horse programs.

    c. Deploying authentication mechanisms wherever technically configurable.

    d. Designing and implementing networks for maximum resiliency.

    e. Developing specific plans for responding to DoS and DDoS attacks in the Company incident management plan and the business continuity plan.

    f. Managing excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

    g. Providing detection and monitoring capabilities to detect indicators of DoS and DDoS attacks against the Company and to determine if sufficient resources exist to prevent effective denial of service attacks.

## D. SC-7: Boundary Protection

1. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with Company security architecture requirements.

    a. Managed interfaces include gateways, routers, firewalls, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

2. Establish a traffic flow policy for each managed interface.

3. Document each exception to the traffic flow policy with a supporting business need and duration of that need.

4. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by an explicit business need.

5. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

6. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal Company network.

7. Limit the number of external network connections to information systems. Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic.

8. Protective controls must, at a minimum, include the following:

    a. Screen internal network addresses from external view

    b. Information systems at managed interfaces must deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

        i. This applies to both inbound and outbound network communications traffic.

        ii. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

9. Web applications should be developed to use a minimum number of ports to allow for easy integration in traditional Demilitarized Zone (DMZ—filtered subnet) environments.

10. Firewalls must be configured to the following specifications:

    a. Local user accounts must be configured on network firewalls for the sole purpose of eliminating possible extended outages.

    b. Local accounts must be configured to only be used when the device cannot contact the central unit.

        i. During normal operation the local account exists but is not used.

    c. Spurious must designate a minimum of two (2) authorized firewall administrators.

i. At least one (1) of the designated firewall administrators will be a security specialist who is consulted before firewall rule set changes are approved and implemented.

d. For temporary or emergency port openings, the Company process must establish a maximum time for the port to be open which must not exceed five (5) days.

i. The Company authorized firewall rule set administrators or the entity managing the firewall must subsequently close the port or develop additional hardening.

e. Firewalls must be installed in locations that are physically secure from tampering.

f. Firewalls must not be relocated without the prior approval of Company management.

g. Firewall rule sets must always block the following types of network traffic:

i. Unauthorized scanning activity that originates outside of its network, within its network, and between information systems.

ii. Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.

iii. Inbound network traffic to the Company's network containing Internet Control Message Protocol (IMCP) traffic will be blocked at the perimeter.

iv. Inbound or outbound network traffic containing a source or destination Internet Protocol (IP) address of 0.0.0.0 or containing directed broadcast addresses or both.

h. Logging features on the Company's network firewalls must capture all packets dropped or denied by the firewall.

i. Company staff or the entity managing the firewall must review those logs at least monthly.

i. Spurious' firewall rule set must be reviewed and verified by Company staff at least quarterly.

j. Firewall configurations and associated documentation must be treated as restricted information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).

11. Information systems in conjunction with a remote device must prevent the device from simultaneously establishing non-remote connections (i.e., split tunneling) with the system and communicating via some other connection to resources on external networks.

### E. SC-8: Transmission Confidentiality and Integrity

1. Spurious must protect confidentiality and integrity of transmitted information to ensure that the confidentiality and integrity of the data is maintained during the transfer process.

2. Spurious must implement safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling.

3. Spurious must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized Company personnel.

4. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic.

5. Spurious must deploy controls to ensure that the Company's resources do not contribute to outside attacks. These controls include the following:

    a. Securing interfaces between Company controlled and non-Company controlled networks or public networks.

    b. Standardizing authentication mechanisms for both users and equipment.

    c. Controlling users' access to information resources.

    d. Monitoring for anomalies or known signatures via Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS).

    e. Intrusion Detection and Prevention System (IDPS) signatures must be up to date.

6. Network users must not intercept or attempt to intercept data transmissions of any kind that they are not authorized to access.

7. Spurious must use secure protocols, such as Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec) for secure network management functions.

8. All communications that transfer confidential sensitive data between web clients and web servers must employ the most current secure transport protocol that includes the most recent version of TLS.

9. Instant messaging technologies, if allowed, must not be used to transmit any type of Restricted or Highly Restricted data.

## F. SC-10: Network Disconnect

1. Spurious must terminate all sessions that have had no activity for a period of thirty (30) minutes or less such that the user must re-authenticate their identity to resume a session.

    a. This control addresses the termination of network connections that are associated with communication sessions (i.e., network disconnect).

## G. SC-12: Cryptographic Key Establishment and Management

1. Spurious must ensure electronic key systems are managed according to the following requirements:

    a. Spurious must use FIPS 140 Level 2 compliant encryption mechanisms when protecting Restricted or Highly Restricted data.

        i. Products and modules that have been validated by NIST as FIPS 140-2 compliant and are currently listed as validated products list may be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

    b. Management is notified of any theft or loss of electronic keys

    c. Cryptographic keys are replaced or retired when keys have reached the end of their life, or the integrity of the key has been weakened or compromised.

    d. Physical protection is employed to protect equipment used to synchronize, store, and archive keys.

## H. SC-13: Cryptographic Protection

1. Spurious must implement cryptographic modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

2. All laptops that are used to access Restricted Data must use encryption to protect all information stored on the laptop's storage device.

3. All other mobile computing devices and portable computing devices such as smart phones, tablets, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and memory sticks (flash drives) that are used to conduct Company business must use encryption to protect all Restricted and Highly Restricted data from unauthorized disclosure.

| Device | Device Encryption Requirements |
|---|---|
| Laptops, Notebooks, etc. | All devices must use Full Disk Encryption (FDE) using a FIPS 140-2 Level 1 certified AES-256 encryption algorithm. |
| Mobile and portable computing devices, such as tablets, smart phones, and personal digital assistants.<br>Removable Media such as CDs, DVDs, memory sticks (flash drives), tape media, or any other portable device that stores data. | All Restricted or Highly Restricted data must be encrypted using a FIPS 140-2 Level 1 certified algorithm of at least a 128-bit strength.<br>**Note:** Restricted and Highly Restricted State data should only be stored on State issued and State-owned media. |

## I. SC-15: Collaborative Computing Devices and Applications

1. Prohibit remote activation of collaborative computing devices such as networked white boards, cameras, and microphones.

2. Provide an explicit indication of use to users physically present at the devices.

a. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

## J. SC-17: Public Key Infrastructure Certificates

1. Spurious must issue Public Key Infrastructure (PKI) certificates or obtain public key certificates from an approved service provider.

2. Registration to receive a public key certificate must include authorization by a responsible official.

3. Public key certificates must be issued using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

## K. SC-18: Mobile Code

1. Spurious must implement security tools, including but not limited to next generation firewalls, anti-virus, anti-malware, and endpoint protection profiles to help mitigate and to provide tamper protection for the Spurious information systems, system components, or information system service to protect the infrastructure from mobile code that performs unauthorized and malicious actions.

2. Spurious must define acceptable and unacceptable mobile code and mobile code technologies.

3. Spurious must review the introduction or modification of mobile code and mobile code technologies within the Company as part of the Change Management and the Technical Review processes to ensure appropriate restrictions and implementation is defined and coordinated.

## L. SC-19: Voice Over Internet Protocol

1. Spurious must establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

2. Spurious must authorize, monitor, and control the use of VoIP within the information system.

3. Transmission of Federal Tax Information by VoIP systems is prohibited.

## M. SC-20: Secure Name/Address Resolution Service (Authoritative Source)

1. Enable external clients, including remote internet clients, to obtain origin authentication and integrity verification assurances for the host or service name to network address resolution information obtained through the service using Domain Name Server (DNS) servers.

2. DNS servers must not be configured to allow zone transfers to unknown secondary servers.

    a. If Spurious maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers.

    b. If Spurious maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only.

    c. When a domain has a US extension (i.e., Spurious.state.nm.us), the US Domain Registry requires the domain to allow copies to be transferred to the US Domain Registry's Master Server.

        i. Therefore, all domains registered with the US Domain Registry will allow transfers of copies of their zones to the Master Server for the US Domain Registry.

## N. SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)

1. Spurious information systems must request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources using recursive resolving or caching DNS servers.

2. Recursion on an authoritative name server is prohibited.

## O. SC-22: Architecture and Provisioning for Name/Address Resolution Service

1. Company information systems that collectively provide name/address resolution service for an Company must be fault tolerant and implement internal/external role separation.

2. At least two (2) authoritative DNS servers must be deployed to eliminate single points of failure and to enhance redundancy.

   a. One configured as the primary server and the other configured as the secondary server or as active/active pair.

3. Servers must be deployed in two (2) geographically separated data centers

4. Servers must be configured to provide redundancy, load balancing and distributed access.

## P. SC-23: Session Authenticity

1. The information system must protect the authenticity of communications sessions.

   a. Spurious must select and implement protection mechanisms to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission.

   b. Mechanisms include but are not limited to ensuring the information system invalidates session identifiers upon user logout or other session termination to curtail the ability of adversaries from capturing and continuing to employ previously valid session IDs.

## Q. SC-28: Protection of Information at Rest

1. Company information systems must protect the confidentiality and integrity of all Restricted or Highly Restricted data at rest.

2. Restricted and Highly Restricted data stored in non-volatile storage (i.e., disk drive) on all endpoints must be encrypted with FIPS 140-2 or National Security Company (NSA) approved encryption compliant encryption during storage regardless of location.

## 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 (CIO)

1. Oversee all technology investments and changes in line with strategic planning and policies set forth in this document.

2. Serve as the final executive authority representing Spurious interests and governance on the Spurious Technical Review Board and the Spurious Change Control Board.

3. Assist Spurious' Chief Information Security Officer (CISO) and IT support staff in understanding their responsibilities and secure training.

4. Ensure that the CISO and IT support staff implement the communication and protection system configurations, components, and tool sets as defined in this document.

### B. Chief Information Security Officer

1. Facilitate implementation of this policy including providing appropriate training to ensure adherence to this policy.

2. Monitor adherence to this policy and report status to the CIO.

3. Assist Spurious personnel in understanding their responsibilities and ensuring that they apply all system configurations, components, and tools sets as defined in this document.

4. Conduct research on emerging technologies and threats and make recommendations for changes to the technology stack and specific information system changes.

### C. IT Infrastructure Technical Manager and Administrators

1. Coordinate the implementation, operations, and maintenance of all communications and protection system configurations, components, and tool sets as defined in this document.

2. Analyze, plan, and implement the partitioning of higher impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described in this document to restrict or prohibit network access and information flow among partitioned information system components in accordance with an organizational assessment of risk.

3. Oversee and manage the creation of PKI framework and services that provide the generation, production, distribution, control, revocation, recovery, and tracking of PKI certificates and their corresponding private keys.

4. Understand, maintain, and support IT infrastructure necessary for the operations of Company business processes.

5. Develop and implement processes, procedures, and standards to ensure compliance with this policy.

6. Maintain daily information system operations.

7. Monitor systems to ensure functional performance is optimal.

## VIII. References

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

NIST SP 800-32 Introduction to Public Key Technology and the Federal PKI Infrastructure must be used as guidance on public key technology.

NIST SP 800-41 Guidelines on Firewalls and Firewall Policy must be used as guidance on firewalls and firewall rule set.

NIST SP 800-52 Guidelines for TLS Implementations must be used as guidance on protecting transmission integrity using TLS and must be used as guidance on the use of TLS mechanisms.

NIST SP 800-54 Border Gateway Protocol Security must be used as guidance on routers.

NIST SP 800-56A Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography and NIST SP 800-56B Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography must be referenced as procedures on establishing cryptographic keys.

NIST SP 800-57 Recommendation for Key Management: Part 1 – General must be referenced as guidance on managing cryptographic keys.

NIST SP 800-61 Computer Security Incident Handling Guide.

NIST SP 800-63, Version 1.0.2 Digital Identity Guidelines must be used as guidance on remote electronic authentication.

NIST SP 800-77 Guide to IPsec VPNs must be used as guidance on Virtual Private Networks (VPNs) and must be used as guidance on protecting transmission integrity using IPsec and must be used as guidance on the deployment of IPsec VPNs and other methods of protecting communications sessions.

NIST SP 800-81 Secure Domain Name System (DNS) Deployment Guide must be used as guidance on DNS message authentication and integrity verification and must be used as guidance on secure domain name system deployment.

NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) must be used as guidance on IDPS.

NIST SP 800-95 Guide to Secure Web Services must be used as guidance on securing web services.

NIST SP 800-113 Guide to SSL VPNs must be used as guidance on SSL VPNs.

NIST as FIPS 140-2 compliant products and modules: http://csrc.nist.gov/groups/STM/cmvp/validation.html.

SPURIOUS PI 603 Code of Conduct Policy

Spurious Change Control Board Charter

Spurious Technical Review Board Charter

## IX. Revision History

| Date | Version | Responsible | Reason for Revision |
|---|---|---|---|
| 16 Dec 2020 | 0.1 | IAO | Initial Draft |
| 11 Jan 2021 | 1.0 | CIO | Final Version |
| 25 July 2022 | 1.1 | IAO | Updated to use Spurious acronym |
| 28 July 2022 | 1.2 | IAO | Added statement to SC-17: Public Key Infrastructure Certificates |
| 31 May 2023 | 1.3 | IAO | Review by Spurious Policy Committee |

## X. Appendices, Forms or Related Material

N/A

## XI. Adoptions

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

_______________________________
Spurious Chief Information Officer

_______________________________
Spurious Chief Executive Officer