UNIVERSITY SYSTEM OF GEORGIA

SUPPLIER MANAGEMENT: A USG IT HANDBOOK COMPANION GUIDE

VERSION 1.0

10/28/2021

PUBLIC

Abstract: This guideline is classified as "Public" and was developed for internal use. The purpose of this guideline is to focus on the elements of supplier management that are directly associated with the management of technology pertaining to cybersecurity and privacy.

REVISION & SIGN-OFF

Change Record

Date	Author	Version	Change Reference

Document Properties

Item	Details
Document Title	Supplier Management: A USG IT Handbook Companion Guide
Document Type	Guideline (Internal Use Only)
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	10/28/2021
Last Updated	10/29/2021
Document Classification	Public

TABLE OF CONTENTS

INTRODUCTION

Protecting USG information and data assets and the systems that collect, process and maintain this data is of critical importance. As a result, USG organizations must implement and manage the security of systems, products and services, which includes control baselines or safeguards to offset possible threats. USG's data protection strategy also includes requirements to ensure the security of data protection controls, regardless of the location or the party responsible for those controls. Suppliers serve a crucial role in achieving this goal. All suppliers are expected to meet the baseline controls identified. If a USG organization permits suppliers to process, store or transmit USG information and data assets that is considered "confidential" or "sensitive," additional data protection controls may be required. Effective cybersecurity is a team effort involving the collaboration, participation and support of each USG organization and its suppliers who interact with USG information and data assets and/or systems.

USG Cybersecurity Practices Alignment

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Privacy Framework represents leading industry-accepted best practices for cybersecurity and data privacy. USG's baseline cybersecurity requirements for its suppliers are consistent with NIST CSF and Privacy controls to ensure due care and due diligence in maintaining its cybersecurity program.

The University System of Georgia (USG) has chosen to align with NIST standards and guidelines in the development of their cybersecurity program. This is intentional as many federal regulations map to NIST. More specifically, the U.S. Department of Education (ED) has mandated that all institutions of higher education entities (IHE) are to demonstrate Gramm-Leach-Bliley Act (GLBA) compliance through the implementation of NIST SP 800-171 Rev1. Failure to demonstrate compliance can result in IHEs losing the ability to administer federal student financial aid. Moreover, the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC) has determined that GLBA compliance is a determining factor for achieving and maintaining accreditation.

CYBERSECURITY RESPONSIBILITIES

USG's requirements for cybersecurity are comprehensive in nature and represent a standard of due care. Suppliers have the same duty of care. Therefore, USG expects suppliers to have a comprehensive set of cybersecurity and privacy policies, standards, procedures and controls to protect USG's information and data assets, as well as its systems, products and services. The requirements apply to all suppliers that support USG operations (e.g., cloud (PaaS, SaaS, and IaaS) suppliers, contractors, consultants, interns or other third parties). This includes all stakeholders involved in accessing, transmitting, processing and storing USG information and data assets. In alignment with the NIST frameworks, the following is a listing of the *Business Procedures Manual* (BPM) and *IT Handbook* (ITHB) safeguards and baseline controls USG organizations should be reviewing when engaging with suppliers.

Identify

Identify focuses on business context; resources that support critical functions; and related cybersecurity and privacy risks. The four controls and the associated mapped responses are:

- *Asset Management* addresses the data, personnel, devices, systems and facilities consistent with the objectives and supplier's risk strategy to protect USG information and data assets.

    - BPM 3.4.4 Supplier Contracts
    - ITHB 5.4 USG Information Asset Management and Protection
    - ITHB 5.6 USG Information Systems Categorization
    - *USG Standard for Supplier Management: Cybersecurity Requirements*

- *Business Environment* informs cybersecurity roles, responsibilities and prioritizes risk management decisions.
    - BPM 12.2 Governance Structure
    - ITHB 5.0 Cybersecurity Charter
    - ITHB 5.5.1 Cybersecurity Program Plan Requirements
    - ITHB 5.2 USG Appropriate Usage Standard
    - ITHB 5.9 Cybersecurity Awareness, Training and Education

- *Governance* addresses the policies, standards, procedures and processes to manage and monitor statutory, regulatory and contractual requirements.
    - BPM 3.4.4 Supplier Contracts
    - BPM 12.2 Governance Structure
    - ITHB 5.0 Cybersecurity Charter
    - ITHB 5.5.1 Cybersecurity Program Plan Requirements
    - ITHB 5.2 USG Appropriate Usage Standard

- *Supplier Risk Management* establishes priorities, constraints, risk tolerances, and assumptions to support decisions associated with managing supplier risk. Exposure due to unauthorized access of USG data or information through a compromised supplier is a risk to the USG for which suppliers have a duty to mitigate.
    - BPM 3.4.4 Supplier Contracts
    - BPM 12.6.2 Data Risk Management
    - ITHB 5.5.1 Risk Assessment and Analysis Requirements
    - ITHB 5.5.3 USG Organization Risk Management Program
    - *USG Standard for Supplier Management: Cybersecurity Requirements*

PROTECT

Protect focuses on cybersecurity awareness and training, and protective technologies. The two controls and the associated mapped responses are:

- *Cybersecurity Awareness and Training* is provided biannual to USG personnel to ensure users are adequately trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
    - BPM 12.5.2 Training
    - ITHB 5.9 Cybersecurity Awareness, Training and Education

- *Protective Technology* solutions are managed to ensure the cybersecurity and resilience of USG systems and assets, consistent with related policies, procedures, and agreements.
    - BPM 3.4.4 Supplier Contracts
    - ITHB 3.1.2 Managing Multifactor Authentication
    - ITHB 5.4 USG Information Asset Management and Protection
    - *USG Standard for Supplier Management: Cybersecurity Requirements*

DETECT

Detect focuses on how incidents can be detected; what constitutes anomalous behavior; and how the systems are being logged & monitored. The three controls and the associated mapped responses are:

- *Continuous Monitoring* addresses the monitoring of information systems to identify cybersecurity events and verify the effectiveness of protective measures.
    - BPM 12.5.3 Monitor
    - ITHB 5.1.3 USG Organizational Responsibilities
    - ITHB 5.1.4 Policy and Procedure Management Requirements
- *Detection Processes* and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
    - ITHB 5.3 Cybersecurity Incident Management
    - ITHB 5.5 Risk Management
    - ITHB 5.8 End Point Security
    - ITHB 5.14 Information Protection Management
- *Anomalies & Events* addresses the detection of anomalous activity and the understanding of potential event impacts.
    - BPM 12.6.5 Data Processing Awareness
    - ITHB 5.1.4 Policy and Procedure Management Requirements

RESPOND

Respond focuses on incident response analysis; and incident response communications. The two controls and the associated mapped responses are:

- *Analysis* evaluates the response and support recovery activities.
    - ITHB 5.1.4 Policy and Procedure Management Requirements
    - ITHB 5.5.1 Risk Assessment and Analysis Requirements
    - ITHB 5.10 Required Reporting
- *Communications* concerning response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
    - BPM 12.4.1 Safeguards
    - ITHB 3.3 Continuity of Operations Planning
    - ITHB 5.0 Cybersecurity Charter
    - ITHB 5.3.4 Cybersecurity Events/Incidents Involving Suppliers

RECOVER

Recover focuses on recovery communications. The control and the associated mapped responses are:

- *Communications* involving restoration activities are coordinated with internal and external parties, USO/ITS/USG Cybersecurity, Internet Service Providers, owners of attacking systems, victims, and incident response teams.
    - BPM 12.4.1 Safeguards

- ITHB 3.3 Continuity of Operations Planning
- ITHB 5.0 Cybersecurity Charter
- ITHB 5.3.4 Cybersecurity Events/Incidents Involving Suppliers
- *USG Standard for Supplier Management: Cybersecurity Requirements*

PRIVACY FRAMEWORK

Data privacy and supplier contract management are interconnected. The privacy framework focuses on inventorying systems, products, and services; privacy risk assessments; and privacy governance requirements. The two controls and the associated mapped responses are:

- *Identify-P* addresses inventory and mapping of the systems, products, and services.
    - BPM 12.6.1 Data Inventory
    - ITHB 6.3.1 Identify-P
    - *USG Standard for Supplier Management: Cybersecurity Requirements*
- *Govern-P* addresses unique requirements concerning privacy governance and documentation; and privacy awareness and training effort.
    - BPM 3.4.4 Supplier Contracts
    - BPM 12.2 Governance Structure
    - ITHB 5.0 Cybersecurity Charter
    - ITHB 5.1 USG Cybersecurity Program
    - ITHB 5.9 Cybersecurity Awareness, Training and Education
    - ITHB 6.3.2 Govern-P

APPENDIX: USG STANDARD FOR SUPPLIER MANAGEMENT: CYBERSECURITY REQUIREMENTS

(2021)

USG requires suppliers that process, transmit or store information and data on behalf of the USG to meet, at a minimum, the standards set forth in this document. Suppliers may also refer to the USG *IT Handbook*[1], a standard that is modeled on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, for additional information.

HIGH RISK: Suppliers are required to protect the availability, integrity and confidentiality of USG information and data assets in the supplier's possession, particularly data classified as "High" risk as defined in USG's *Business Procedures Manual*, Section 3.4.4[2]. Examples of the information and data that trigger a "High" classification include but are not limited to USG's mission-critical systems, personally identifiable information ("PII") such as date of birth, social security number, names of minor children, health information, financial information (credit card numbers, bank account numbers), student records as defined by FERPA, etc. To ensure that USG suppliers provide for the integrity and cybersecurity of USG's "high risk" information and data assets as required, USG requires its suppliers to:

1. Implement and maintain management and staff accountability for the protection of USG information and data assets. As part of this program, the Supplier shall ensure management and staff receive annual cybersecurity awareness training.
2. Establish and maintain risk management practices to meet USG's program objectives in the event of the unavailability, loss or misuse of USG information and data assets. Also, the Supplier must:
    a) Establish and maintain processes for the assessment and analysis of risks associated with USG information and data assets;
    b) Implement Intrusion Prevent System (IPS)/firewall configurations to detect anomalous activity in a timely manner to understand potential impacts. The Supplier shall document the baseline configuration each IPS/firewall with dataflow diagrams, update the documentation with all authorized changes and conduct periodic verification of the configuration; and
    c) Architect network segmentation, or an equally effective measure, to isolate USG information and data assets as a cybersecurity safeguard.
3. Establish and maintain processes to identify and report cybersecurity incidents affecting USG information and data assets. Suppliers must promptly report all cybersecurity incidents or events of interest affecting systems or data for any of the cybersecurity objectives of confidentiality, integrity or availability to USG Cybersecurity through the Enterprise Service Desk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3697 (Toll free within Georgia). Further, suppliers should also notify the USG point of contact as identified in their contract.
4. Develop and implement a vulnerability management plan that includes, but is not limited to:

[1] https://www.usg.edu/information_technology_services/it_handbook/

[2] https://www.usg.edu/business_procedures_manual/

a) Continuous monitoring to identify and verify the effectiveness of implemented protective measures, e.g. vulnerability scanning, and

b) Security patches and security upgrades, which include, but are not limited to, servers, routers, desktop computers, mobile devices and firewalls. Application and testing of the patches and/or security upgrades must be addressed.

5. Technology upgrades, which include, but are not limited to, operating system upgrades on servers, routers and firewalls. Appropriate planning and testing of upgrades must be addressed.

    a) Server configurations includes all servers that have any interaction with the Internet (public facing) or intranet traffic that manages USG information and data assets. Document the baseline configuration for each server with dataflow diagrams, update the documentation with all authorized changes and conduct periodic verification of the configuration.

    b) Server hardening must cover all servers that manages USG information and data assets. The process for making changes based on newly published vulnerability information as it becomes available must be included. Principles of least functions must be implemented.

6. Software management and software licensing must address acquisition from reliable and safe sources and must clearly state that using pirated or unlicensed software is prohibited.

7. Data files that are downloaded/uploaded must meet information and data integrity and cybersecurity protective safeguards (e.g., user access, rights and privileges), which were established for the original data file and which must be applied in the new environment.

8. Encryption, or an equally effective measures, is required for all personal, sensitive or confidential information that is processed (in-use), transmitted (in-transit) and stored (at-rest).

MODERATE RISK: USG shall require suppliers to protect the availability and integrity of the information and data assets classified as “Moderate” risk as defined in USG’s *Business Procedures Manual*, Section 3.4.4 that includes but are not limited to publicly available information, directory information, and non-confidential information. Additionally, incident reporting as stated in item three (of this document) is also required.

LOW RISK: USG shall require suppliers to protect the availability of the systems, products or services classified as “Low” risk as defined in USG’s *Business Procedures Manual*, Section 3.4.4. Additionally, incident reporting as stated in item three (of this document) is also required.

NONE: No Cybersecurity review is required – no systems, products, services and/or USG data are being exchanged as part of the contract.