Security Assessment and Attestation

Introduction

[Company Name] business units often engage external service providers for information processing and services to supplement or augment our capabilities. It is important for the Information Owner to be able to assess risks related to external service providers, and to understand how information is adequately protected wherever it is being processed and/or stored.

Service provider is encouraged to provide evidence of the claims and/or attestations of security controls described herein. [Company Name] business units reserve the right to validate the effectiveness of the security controls described herein. Nothing contained herein shall be construed to limit any of Service Provider's obligations regarding agreements with [Company Name] business units.

Assessment & Attestation Information

Date of Assessment & Attestation	
Facility or Organization Name	
Facility Address:	
Facility City, State, Zip Code:	
Contact Name:	
Contact Phone Number:	
Contact Email Address:	
Attestor Title	
Attestor Name	
Attestor Signature	

Definitions

Attestor: Individual who confirmed and/or witnessed the truthfulness of the claims and/or assertions herein.

Business Unit: A [Company Name] entity engaging external service provider for information processing and services.

Service Provider: A non-[Company Name] entity that provides to [Company Name] or affiliated business unit a service, product or combination thereof requiring information management, data processing and/or storage of [Company Name] Information.

Security Assessment: A process of examining the security posture of an organization and/or facility(ies) and determining its ability to continue proper operation in the face of adversity. Assessments are used to identify gaps in security controls which will then be addressed during subsequent work.

System: software, hardware, equipment, etc. that may exist in the service provider network or at customer premises.

Instructions

Each question focuses on a specific area of security. In the answer section, please provide references to documents and evidence attesting to the processes and tools used to meet the security objective. Attestation is service provider's self-certification that you are capable of meeting and/or exceeding the security objective.

All information disclosed in this document and supporting documentation will be classified as confidential. Transmission of this information should use [DESCRIBE CONFIDENTIAL MEANS OF DISCLOSURE]

Please print the first page, have Attestor sign, and include a scanned copy as part of the electronic package submitted.

Questionnaire

[Company Name] Business Unit and Information Security would like to learn more about the security characteristics of external service provider that are provided now or will be provided in the future.

Independent Assessments

Service Organization Controls

Has your facility been audited for service organization controls, such as SOC 2 / SSAE 16? If yes, please provide most recent report. If an audit of service organization controls is not applicable, please explain why.

Answer:	

Information Security Framework

Has your facility been audited for compliance with an information security framework, such as ISO/IEC 27001? If yes, please provide most recent report. If compliance with a security framework is not applicable, please explain why.

Answer:	

Independent Cyber Security Assessment

Has your infrastructure, including the hosted applications, been security tested by independent cybersecurity firm? If yes, please provide most recent report. If security testing by independent cybersecurity firm is not applicable, please explain why.

Answer:	

Security Assessment and Attestation

Inventory of Authorized and Unauthorized Devices

Describe and attest to the processes and/or tools used to monitor/control/prevent/correct network access by devices (computers, network components, printers, tablets, mobile phones and anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Inventory of Authorized and Unauthorized Software

Describe and attest to the processes and/or tools your organization uses to monitor/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Describe and attest to the processes and/or tools your organization uses to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Continuous Vulnerability Assessment and Remediation

Describe and attest to the processes and/or tools used to detect/prevent/correct security vulnerabilities in the configurations of devices that are listed and approved in the asset inventory database. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Malware Defenses

Describe and attest to the processes and/or tools used to detect/prevent/correct installation and execution of malicious software on all devices. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Application Software Security

Describe and attest to the processes and/or tools your organization uses to detect/prevent/correct security weaknesses in the development and acquisition of software applications. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Wireless Device Control

Describe and attest to the processes and/or tools used to monitor/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Data Recovery Capability

Describe and attest to the processes and/or tools used to properly back up critical information with a proven methodology for timely recovery of it. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Security Skills Assessment and Appropriate Training to Fill Gaps

Describe and attest to the processes and/or tools your organization uses to assess understands the technical cybersecurity skills within your workforce, including processes and/or tools to fill the gaps through policy, training, and awareness. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Describe and attest to the processes and/or tools used to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Limitation and Control of Network Ports, Protocols, and Services

Describe and attest to the processes and/or tools used to track/control/prevent/correct use of ports, protocols, and services on networked devices. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Controlled Use of Administrative Privileges

Describe and attest to the processes and/or tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Boundary Defense

Describe and attest to the processes and/or tools used to detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Maintenance, Monitoring, and Analysis of Audit Logs

Describe and attest to the processes and/or tools used to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of the organization. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Controlled Access Based on the Need to Know

Describe and attest to the processes and/or tools used to track/control/prevent/correct secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information based on an approved classification. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Account Monitoring and Control

Describe and attest to the processes and/or tools used to track/control/prevent/correct the use of system and application accounts. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Data Loss Prevention

Describe and attest to the processes and/or tools used to track/control/prevent/correct data transmission and storage, based on the data's content and associated classification. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Incident Response and Management

Describe and attest to the processes and/or tools to assure your organization has a properly tested incident response plan with appropriately trained resources for dealing with any adverse events or threats of adverse events. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Secure Network Engineering

Describe and attest to the processes and/or tools used to build, update, and validate a network infrastructure that can properly withstand attacks from advanced threats. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	

Penetration Tests and Red Team Exercises

Describe and attest to the processes and/or tools used to simulate attacks against your infrastructure (servers, applications, network devices, etc.) to validate the overall security of your organization. Please explain if security objective not applicable to organization, or if compensating controls used to meet security objective.

Answer:	