DoProcess Unity®

Unity®

Security & Technical Implementation Guide

Version 1.4

November 4, 2019

DoProcess Unity®

Security & Technical Implementation Guide

Introduction and scope of this document

At DoProcess the integrity, confidentiality and availability of our customers' data is a primary focus. Unity is designed to help legal practices streamline the operation of their business. Securely hosted by DoProcess on a private cloud, Unity was built from the ground up with security in mind to protect your clients' information and firm data.

This document summarizes all security policies, procedures and guidelines implemented by DoProcess to ensure Unity data and information resources are protected against the possibility of loss due to accidental or natural causes, misuse, misappropriation or disclosure.

DoProcess Unity®

Table of contents

1

Risk Management Framework, Controls & Certifications

DoProcess has a documented approach to risk assessment. The program integrates multiple security practices and procedures to help us identify and mitigate risk to its critical IT assets – including Unity – and then assists in maintaining an optimal security posture across the enterprise.

Control objectives and controls selected from annex A of ISO27001, COBIT, PCI DSS and industry-accepted best practices provide DoProcess with confidence and assurance that its mission-critical business systems, networks, applications and physical environments are protected against threats.

Since risks and threats change over time, DoProcess periodically reviews the appropriateness and effectiveness of the policies and controls implemented.

A “risk register” is regularly provided to DoProcess’ board of directors and any issues requiring remediation are tracked by our internal dedicated security team requiring weekly progress until remediated. See section 10, Unity Incident Event Management & Compliance for additional information.

2

DoProcess Corporate Security Policies & Organizational Security

DoProcess is committed to security and all documented corporate security policies apply to Unity. It is the policy of DoProcess to protect our assets and ensure;

- the confidentiality and security of DoProcess, its assets and its staff,
- the continued, uninterrupted operation of DoProcess;
- the use of all assets is for purposes authorized by DoProcess

Unity assets are subject to monitoring, inspection and examination in order to protect the interests of DoProcess, our business partners and staff. *Restricted,* and *Private and Confidential* DoProcess information is available to individuals on a need-to-know basis. Attempts to access information or the use of information resources outside one's authority are not condoned and may lead to suspension, termination and/or legal action.

DoProcess has defined, documented information security responsibilities for specific information security procedures. There is a dedicated security operations team overseeing that all applications – including Unity – adhere to DoProcess corporate security policies.

All DoProcess security policies are endorsed and approved by senior management *and* a dedicated security committee which supports the management of information security and enforcement of security policy within DoProcess. Security policies are communicated to all staff and third-party contractors, and there are mechanisms in place to ensure compliance.

3

Unity Organization of Information Security

All DoProcess staff and contractors who work on Unity must agree to background and security checks and to follow all DoProcess information security policies before they are authorized to access Unity assets. Annually thereafter, all employees are required to acknowledge that they have reviewed, understand and agree to comply with the DoProcess Security Code of Conduct.

Every employee must attend mandatory information security awareness class or computer-based training annually after starting with DoProcess.

DoProcess' process for managing Unity information security and its implementation (i.e. control objectives, controls, policies, rules, processes and procedures for information security) is independently reviewed at planned intervals, and when significant changes to the security implementation occur.

4

Unity Asset Management & Information Classification Guidelines

All Unity information assets have been identified, and the security processes associated with each asset have been defined following a risk assessment and documented.

Unity assets are classified, labelled (private and confidential, highly restricted, restricted, internal use, public or external) and documented to enforce segregation of duties. All Unity assets have custodians whose responsibility for the day-to-day maintenance of the controls applied to these assets and are documented.

5

Unity Human Resources Security

DoProcess maintains a documented human resources security policy as part of our corporate recruitment process. Whether staff are hired on a full-time, part-time, temporary, or contractual basis – the corporate recruitment process is followed.

All permanent and non-permanent employees are screened prior to employment. These screenings include criminal and credit checks, employment reference verification, education and credential verification.

Permanent and non-permanent employees are required to sign any agreements that pertain to non-disclosure, confidentiality and information security policies.

6

Unity Physical & Environmental Security

Unity is hosted in a Tier 3 data centre owned and operated by DoProcess' parent company, and no data hosting or processing is outsourced to a third party. Data centres are restricted to authorized personnel only. Data centres are free of readily identifiable signs and other indications that reveal the existence of the data centre.

Access to data centres and offices is logged, including the time of entry and exit, and visitors are escorted at all times. Closed-circuit television monitoring (CCTV) is installed in sensitive areas, which are monitored 24/7 by a qualified professional security team.

Are all Unity assets that are added/removed from data centres (i.e. backups) are logged and approved by management and vendors.

Data centres have robust environmental controls to monitor and control heat, humidity, fire suppression, emergency lighting and uninterrupted power supply (UPS).

7

Unity Communications & Operations Management

Unity is supported, hosted and maintained exclusively by DoProcess. We maintain documented policies to ensure the correct and secure operation of information processing at our facilities.

DoProcess follows best practices regarding the configuration of firewalls, network devices, DMZ, servers, workstations, laptops and mobile devices including multiple zones (protected with multiple firewall solutions), dedicated DMZ as well as “zero-trust networking”.

DoProcess adheres to the ITIL framework for formal change management/change control processes. Firewall changes performed via this change control process can only be performed by a restricted number of authorized individuals.

The DoProcess Unity production environment operates on hardware on an isolated network which is firewalled from all other environments. Client/customer data is isolated from all DoProcess company data. Any remote access requires VPN connectivity enforcing both an encrypted channel and multifactor authentication.

Unity customer data resides where the Unity application requires it. Storage is contained to a small number of databases within the data center.

Robust monitoring solutions are in place as well as network controls to restrict access from a range of data loss vectors.

Data is backed up regularly daily with the ability to recover to any point in time. Data verification is done quarterly. The only form of removable media is encrypted removable media used for backups.

DoProcess maintains regular patch cycles to ensure patches are applied within 30 days. All endpoints have up-to-date, monitored virus protections.

8

Unity Access controls

Robust controls are in place for authentication, authorization and monitoring access to Unity.

All customers are required to provide their firm account ID, unique user ID and password to access Unity. Passwords need to adhere to DoProcess' strong password policy which requires all passwords to have a minimum of 8 characters containing characters from at least three of the following groups: uppercase letters, lowercase letters, numbers and special characters. Accounts are locked following five unsuccessful authentication attempts. Users must not use passwords that are identical to passwords they previously used in the last five passwords.

Users are forced to change their password every 90 days.

All access to Unity is logged (including privileged accounts) and monitored. DoProcess reviews all Unity security event logs daily and as required.

Only Unity customers have access to Unity customer data as per DoProcess policies.

For additional security, Unity uses two-step authentication (AKA two-factor authentication or 2FA). Two-factor authentication is enforced by DoProcess IT operation management within the Unity environment.

9

Unity Cloud Services, Encryption & Compatibility

Unity and all Unity data are securely hosted on DoProcess owned, operated and maintained servers located in Canada. No customer data is stored on firm local network or computers.

Access to Unity is completely web-based, and Unity does not require any special software to be installed on local user computers. Unity is access by all supported versions of popular web browsers, including Internet Explorer (11+) and Chrome (63+). DoProcess provides a dedicated Unity Minimum Requirements Checker to make sure your work-station is up to date and meets all minimum requirements for Unity.

All data to and from Unity is encrypted in transit. At rest, the application only encrypts data that is deemed sensitive. Current client birthdates and identification card details are encrypted in the database. Additionally, all documents created by or loaded into the Unity system are encrypted. Encryption keys are stored on a secure database server only accessible by authorized senior database staff. Encryption keys are changed on a yearly basis.

10

Unity Incident Event Management & Compliance

DoProcess maintains a documented plan for the management of any potential Unity information security event which details procedures to ensure information and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. Our incident response plan follows an incident lifecycle framework which clearly outlines steps from detection and response to reporting, recovery, remediation and review.

DoProcess complies with all applicable federal and provincial data privacy, data security, confidentiality, consumer protection, advertising, electronic mail, data destruction and other similar laws, rules, and regulations relating to the privacy and security of personal information. In the unlikely event of a data breach DoProcess will work cooperatively with our clients to ensure compliance with all applicable laws.

11

Unity Business Continuity & Disaster Recovery Management

DoProcess maintains documented business continuity plans, including comprehensive disaster recovery strategies for Unity. These plans are updated annually. Exercises to simulate various DR scenarios are executed yearly to validate and improve our BCP and DR plans and strategies. All DoProcess BCP and Unity DR plans are reviewed and approved by senior DoProcess management yearly.

Unity Application Security Features

Access Groups

This feature allows a firm to restrict user access to only certain matters. Administrators can identify groups of users that will have access to certain matters. When a new matter is opened, staff can choose what access group can access that specific file. This limits disclosure in the event of unauthorized access.

Access profiles

Access profiles restrict individual user access to certain application functionality (matters, billing, client contacts) and the type of access (read, write or no access). This limits access and allows firms greater flexibility.

Two Factor Authentication

Authentication does not happen at every login. It only occurs in one of the following scenarios:

- User logs in for the first time
- User logs into Unity from a new computer (users can designate trusted devices, so they don't need to enter the code on subsequent logins)
- User "resets " a forgotten password.
- It has been three months since the user's last login

In addition, each user can specify more than one trusted cell number. The Unity application also allows administrative users from your firm to generate a code in the event that a user in your firm forgot or lost their phone.

Email Notifications

Firm administrators are provided notifications in the following scenarios:

- Changes are made to their account details
- New users are created on their account
- New users' login for the first time

User Management

The Unity application provides the following user management features:

- Lockout on more than five failed log-in attempts
- Administrator ability to suspend users
- 3-month password expiry

13

Unity Security and Technical Implementation FAQ

Risk Assessment & Treatment

Q

Is there a formalized Risk Governance plan and a continuous Risk Assessment program that identifies, quantifies, and prioritizes risks based on the risk acceptance levels relevant to the organization?

A

Yes, there is a formalized Risk Governance plan and a continuous Risk Assessment program that identifies, quantifies, and prioritizes risks based on the risk acceptance levels relevant to the organization

Q

Does the formalized Risk Governance plan and a continuous Risk Assessment program that identifies, quantifies, and prioritizes risks based on the risk acceptance levels include risk management policies, procedures, and internal controls?

A

Yes, the formalized Risk Governance plan and a continuous Risk Assessment program includes risk management policies, procedures, and internal controls

Q

Is there a program to manage the treatment of identified risks?

A

Yes, there is a program to manage the treatment of identified risks

Q

Do subcontractors have access to Scoped Systems and Data or processing facilities?

A

No, Subcontractors do not have access to Scoped Systems and Data or processing facilities

Security Policy

Q

Is there a set of information security policies that have been approved by management, published, and communicated to Constituents?

A

Yes, there is a set of information security policies that have been approved by management, published, and communicated to Constituents

Q

Have all policies been assigned to an owner responsible for review and approval periodically?

A

Yes, all policies have been assigned to an owner responsible for review and approval periodically

Q

Have all information security policies and standards been reviewed in the last 12 months?

A

Yes, all information security policies and standards have been reviewed in the last 12 months

Q

Is the maturity of IT management processes formally evaluated at least annually using an established benchmark?

A

Yes, the maturity of IT management processes have been formally evaluated at least annually using an established benchmark (e.g. COBIT maturity models)

Organizational Security

Q

Are responsibilities for asset protection and for carrying out specific information security processes clearly identified and communicated to the relevant parties?

A

Yes, the responsibilities for asset protection and for carrying out specific information security processes clearly identified and have been communicated to the relevant parties

Q

Do all projects involving Scoped Systems and Data go through some form of information security assessment?

A

Yes, all projects involving Scoped Systems and Data go through some form of information security assessment

Q

Are information security personnel (internal or outsourced) responsible for information security processes?

A

Yes, information security personnel are responsible for information security processes

Q

Are information security personnel (internal or outsourced) responsible for the creation and review of information security policies?

A

Yes, information security personnel (internal or outsourced) are responsible for the creation and review of information security policies

Q

Are information security personnel (internal or outsourced) responsible for the review and/or monitoring of information security Incidents or events?

A

Yes, information security personnel (internal or outsourced) are responsible for the review and/or monitoring of information security incidents or events

Asset Management and Information Management

Q

Is there an Asset Management Program approved by management, communicated to constituents and an owner to maintain and review?

A

Yes, there is an Asset Management Program that is approved by management, communicated to constituents and an owner to maintain and review it

Q

Is there an asset Inventory list or Configuration Management Database (CMDB)?

A

Yes, there is an asset Inventory list or Configuration Management Database (CMDB)

Q

Is there an 'Acceptable Use Policy' for information and associated assets that has been approved by management, communicated to appropriate constituents and assigned an owner to maintain and periodically review the policy?

A

Yes, there is an 'Acceptable Use Policy' for information and associated assets that has been approved by management, communicated to appropriate constituents and assigned an owner to maintain and periodically review the policy

Q

Is there a process to verify return of constituent assets upon termination?

A

Yes, there is a process to verify return of constituent assets upon termination

Q

Is Information classified according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification?

A

Yes, information is classified according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification

Q

Is an owner assigned to all Information Assets?

A

Yes, there is an owner assigned to all Information Assets

Q

Are owners responsible to approve and periodically review access to Information Assets?

A

Yes, owners are responsible to approve and periodically review access to Information Assets

Q

Is there a policy or procedure for information handling consistent with its classification that has been approved by management, communicated to appropriate constituents and assigned an owner to maintain and periodically review?

A

Yes, there is a policy or procedure for information handling consistent with its classification that has been approved by management, communicated to appropriate constituents and assigned an owner to maintain and periodically review

Q

Are encryption requirements included within the policy or procedure for information handling?

A

Yes, encryption requirements are included within the policy or procedure for information handling

Q

Are storage requirements, including authorized use of Public Cloud storage, included within the policy or procedure for information handling?

A

Yes, storage requirements are included within the policy or procedure for information handling

Q

Are electronic transmission security requirements (including email, web, and file transfer services) included within the policy or procedure for information handling?

A

Yes, electronic transmission security requirements are included within the policy or procedure for information handling

Q

Are removable media requirements included within the policy or procedure for information handling?

A

Yes, removable media requirements are included within the policy or procedure for information handling

Q

Are data retention/destruction requirements that include information on live media, backup/archived media, and information managed by Subcontractors included within the policy or procedure for information handling?

A

Yes, data retention/destruction requirements are included within the policy or procedure for information handling

Q

Is Scoped Data sent or received via Physical Media?

A

No, Scoped Data is not sent or received via Physical Media

Q

Is Scoped Data sent or received electronically?

A

Yes, Scoped Data is sent or received electronically

Q

Is 'encryption in transit' utilized while sending or receiving Scoped Data outside the network?

A

Yes, 'encryption in transit' is utilized when sending or receiving Scoped Data outside the network

Q

Is there protection against malicious code by utilizing network virus inspection or virus scans at the endpoint?

A

Yes, there is protection against malicious code by utilizing network virus inspection or virus scans at the endpoint

Q

Is regulated or confidential Scoped Data stored electronically?

A

Yes, regulated or confidential Scoped Data is stored electronically

Q

Is regulated or confidential Scoped Data stored in a database?

A

Yes, regulated or confidential Scoped Data is stored in a database

Q

Is regulated or confidential Scoped Data stored in files?

A

No, regulated or confidential Scoped Data is not stored in files

Q

Are encryption keys managed and maintained for Scoped Data?

A

Yes, encryption keys are managed and maintained for Scoped Data

Q

Are the encryption keys generated in a manner consistent with key management industry standards?

A

Yes, encryption keys are generated in a manner consistent with key management industry standards

Q

Is there an option for clients to manage their own encryption keys?

A

No, there are no options for clients to manage their own encryption keys

Q

Are constituents able to view client's unencrypted Data?

A

No, constituents are not able to view client's unencrypted Data

Human Resources Security

Q

Are there Human Resource policies approved by management, communicated to constituents and an owner to maintain and review?

A

Yes, there are Human Resource policies approved by management, communicated to constituents and an owner to maintain and review

Q

Do Human Resource policies include constituent background screening criteria?

A

Yes, Human Resource policies do include constituent background screening criteria

Q

Does constituent background screening criteria include criminal checks?

A

Yes, constituent background screening criteria includes criminal checks

Q

Do Human Resource policies include security awareness training?

A

Yes, Human Resource policies include security awareness training

Q

Does security awareness training include security roles and responsibilities?

A

Yes, security awareness training includes security roles and responsibilities

Q

Does security awareness training include new hire and annual participation?

A

Yes, security awareness training includes new hire and annual participation

Q

Do Human Resources polices include a disciplinary process for non-compliance?

A

Yes, Human Resources polices do include a disciplinary process for non-compliance

Q

Do Human Resources polices include a termination and/or change of status process?

A

Yes, Human Resources polices include a termination and/or change of status process

Q

Is electronic access to systems containing Scoped Data removed within 24 hours for terminated constituents?

A

Yes, electronic access to systems containing Scoped Data is removed within 24 hours for terminated constituents

Physical and Environmental Security

Q

Is there a physical security program approved by management, communicated to constituents, and has an owner assigned to maintain and review?

A

Yes, there is a physical security program approved by management, communicated to constituents, and has an owner assigned to maintain and review

Q

Does the physical security program include physical access and environmental controls?

A

Yes, the physical security program include physical access and environmental controls

Q

Does the physical security program include physical security and environmental controls in the data center and office buildings?

A

Yes, the physical security program includes physical security and environmental controls in the data center and office buildings

Q

Do the physical security and environmental controls in the data center and office buildings include restricted access and are logs kept of all access?

A

Yes, the physical security and environmental controls in the data center and office buildings include restricted access and logs are kept of all access

Q

Do the physical security and environmental controls in the data center and office buildings include electronic controlled access system (key card, token, fob, Biometric Reader, etc.)?

A

Yes, physical security and environmental controls in the data center and office buildings include an electronic controlled access system

Q

Do the physical security and environmental controls in the data center and office buildings include alarmed entry and exit doors (forced entry, propped open) and/or monitoring by security guards?

A

Yes, the physical security and environmental controls in the data center and office buildings include alarmed entry and exit doors (forced entry, propped open) and/or monitoring by security guards

Q

Do physical access control procedures exist?

A

Yes, physical access control procedures exist

Q

Do physical access procedures include the collection of access equipment (badges, keys, change pin numbers, etc.) upon termination or Status Change?

A

Yes, physical access procedures include the collection of access equipment (badges, keys, change pin numbers, etc.) upon termination or Status Change

Q

Do physical access procedures include lost or stolen access card/key reporting requirements?

A

Yes, physical access procedures include lost or stolen access card/key reporting requirements

Q

Are visitors permitted in the facility?

A

Yes, visitors are permitted in the facility

Q

Do the Scoped Systems and Data reside in a data center?

A

Yes, Scoped Systems and Data reside in a data center

Q

Are locking screensavers on unattended system displays or locks on consoles required within the data center?

A

Yes, locking screensavers on unattended system displays or locks on consoles are required within the data center

Q

Is there a procedure for equipment removal from the data center?

A

Yes, there is a procedure for equipment removal from the data center

Organization Management

Q

Are management approved operating procedures utilized?

A

Yes, management approved operating procedures are utilized

Q

Is there an operational change management/Change Control policy or program that has been documented, approved by management, communicated to appropriate constituents and assigned an owner to maintain and review the policy?

A

Yes, there is an operational change management/change control policy or program that has been documented, approved by management, communicated to appropriate constituents and assigned an owner to maintain and review the policy

Q

In the operational change management/change control policy or program, are changes to the production environment including network, systems, application updates, and code changes subject to the change control process?

A

Yes, changes to the production environment including network, systems, application updates, and code changes subject to the change control process

Q

In the operational change management/change control policy or program, is there a formal process to ensure clients are notified prior to changes being made which may impact their service?

A

Yes, there is a formal process to ensure clients are notified prior to changes being made which may impact their service

Q

In the operational change management/change control policy or program, is there a scheduled maintenance window?

A

Yes, there is a scheduled maintenance window

Q

In the operational change management/change control policy or program, does the scheduled maintenance window which results in client downtime?

A

Yes, there is a scheduled maintenance window which results in client downtime

Q

Are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced?

A

Yes, there are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced

Q

When new systems are introduced, upgraded, or enhanced, is a determination of security requirements based on the sensitivity of the data included?

A

Yes, a determination is made of security requirements based on the sensitivity of the data

Q

Do systems and Network Devices utilize a common time synchronization service?

A

Yes, systems and network devices utilize a common time synchronization service

Access controls

Q

Does the password policy for systems that transmit, process or store scoped systems and data, require keeping passwords confidential?

A

Yes, passwords are kept confidential

Q

Does the password policy for systems that transmit, process or store scoped systems and data, state users are not to keep a record of passwords (paper, software file or handheld device)?

A

Yes, the password policy state users are not to keep a record of passwords (paper, software file or handheld device)

Q

Does the password policy for systems that transmit, process or store scoped systems and data, require passwords be changed when there is an indication of possible system or password compromise?

A

Yes, passwords are changed when there is an indication of possible system or password compromise

Q

Does the password policy for systems that transmit, process or store scoped systems and data, require changing passwords at regular intervals?

A

Yes, passwords are changed at regular intervals

Q

Does the password policy for systems that transmit, process or store scoped systems and data, require users terminate or secure active sessions when finished?

A

Yes, users are required to terminate or secure active sessions when finished

Q

Does the password policy for systems that transmit, process or store scoped systems and data, state users are to logoff terminals, PC or servers when the session is finished?

A

Yes, users are to logoff terminals, PC or servers when the session is finished

Q

Does the password policy for systems that transmit, process or store scoped systems and data, prevent the inclusion of unencrypted passwords in automated logon processes (e.g., stored in a macro or function key)?

A

No, unencrypted passwords are not included in automated logon processes (e.g., stored in a macro or function key)

Q

Does the password policy for systems that transmit, process or store scoped systems and data, permit a PIN or secret question as a possible stand-alone method of authentication?

A

No, a pin or secret question is not a possible stand-alone method of authentication

Q

Are passwords encrypted in transit?

A

Yes, passwords are encrypted in transit

Q

Are passwords encrypted or hashed in storage?

A

Yes, passwords are encrypted or hashed in storage

Q

Is password reset authority restricted to authorized persons and/or an automated password reset tool?

A

Yes, a password reset authority is restricted to authorized persons and/or an automated password reset tool

Q

Are user IDs and passwords communicated/distributed via separate media (e.g., e-mail and phone)?

A

Yes, user IDs and passwords are communicated/distributed via separate media (e.g., e-mail and phone)

Q

Is Remote Access permitted?

A

Yes, remote Access is permitted

Q

Are encrypted communications required for all remote connections?

A

Yes, encrypted communications are required for all remote connections

Q

Are Constituents able to access Scoped Data?

A

Yes, constituents are able to access Scoped Data

Application Security

Q

Are applications used to transmit, process or store Scoped Data?

A

Yes, applications are used to transmit, process or store Scoped Data

Q

For applications used to transmit, process or store scoped data, are outside development resources utilized?

A

Yes, outside development resources are utilized

Q

For applications used to transmit, process or store scoped data, are system, vendor, or service accounts disallowed for normal operations and monitored for usage?

A

Yes, system, vendor, or Service Accounts are disallowed for normal operations and monitored for usage

Q

For applications used to transmit, process or store scoped data, are web applications configured to follow best practices or security guidelines (e.g., OWASP)?

A

Yes, web applications are configured to follow best practices or security guidelines (e.g., OWASP)

Q

For applications used to transmit, process or store scoped data, is data input into applications validated?

A

Yes, data is input into applications validated

Q

For applications used to transmit, process or store scoped data, are scoped systems and data used in the test, development, or QA environments?

A

No, scoped systems and data are not used in the test, development, or QA environments

Q

Is application development performed?

A

Yes, application development is performed

Q

Does application development use a formal Software Development Life Cycle (SDLC) process?

A

Yes, there is a formal Software Development Life Cycle (SDLC) process

Q

Is there a secure software development lifecycle policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?

A

Yes, there is a secure software development lifecycle policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy

Q

For developed applications, is there a documented change management/change control process?

A

Yes, there is a documented change management/change control process

Q

For developed applications, are the change control procedures required for all changes to the production environment?

A

Yes, change control procedures are required for all changes to the production environment

Q

For developed applications, does the change control policy require testing prior to deployment?

A

Yes, there is testing prior to deployment

Q

For developed applications does the change control procedures require stakeholder communication and/or approvals?

A

Yes, there is stakeholder communication and/or approvals

Q

For developed applications does the change control procedures require documentation of all system changes?

A

Yes, there is a documentation for all system changes

Q

For developed applications does the change control procedures require version control for all software?

A

Yes, there is version control for all software

Q

For developed applications does the change control procedures require logging of all change requests?

A

Yes, there is logging of all change requests

Q

For developed applications, are they evaluated from a security perspective prior to promotion to production?

A

Yes, applications are evaluated from a security perspective prior to promotion to production

Q

For developed applications, is an open source software or library used to transmit, process or store scoped data?

A

Yes, there is open source software or library used to transmit, process or store scoped data

Q

For developed applications, is a secure code review performed regularly?

A

Yes, a secure code review is performed regularly

Q

For developed applications, is a regular analysis of vulnerability to recent attacks performed?

A

Yes, there is regular analysis of vulnerability to recent attacks

Q

For developed applications, are identified security vulnerabilities remediated prior to promotion to production?

A

Yes, identified security vulnerabilities are remediated prior to promotion to production

Q

For developed applications, is known unremediated vulnerabilities communicated to the security monitoring and response group for awareness and monitoring?

A

Yes, unremediated vulnerabilities are communicated to the security monitoring and response group for awareness and monitoring

Q

Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?

A

Yes, a web site is supported, hosted or maintained that has access to Scoped Systems and Data

Q

For web sites supported, hosted or maintained that has access to scoped systems and data, do you have logical or Physical segregation between web, application and database components? i.e., Internet, DMZ, Database?

A

Yes, there is logical or physical segregation between web, application and database components

Q

Are web servers used for transmitting, processing or storing scoped data?

A

Yes, web servers are used for transmitting, processing or storing scoped data

Q

Web servers used for transmitting, processing or storing scoped data, are reviews performed to validate compliance with documented standards?

A

Yes, reviews are performed to validate compliance with documented standards

Q

Web servers used for transmitting, processing or storing scoped data, is HTTPS enabled for all web pages?

A

Yes, HTTPS is enabled for all web pages

Q

Web servers used for transmitting, processing or storing scoped data, are sample applications and scripts removed?

A

Yes, sample applications and scripts are removed

Q

Web servers used for transmitting, processing or storing scoped data, are available high-risk security patches applied and verified at least monthly?

A

Yes, available high-risk security patches are applied and verified at least monthly

Q

Web servers used for transmitting, processing or storing scoped data, is there prohibition of versions that no longer have patches released?

A

Yes, there is prohibition of versions that no longer have patches released

Q

For web servers used for transmitting, processing or storing scoped data, is sufficient detail contained in web server and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?

A

Yes, sufficient details are contained in web server and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files

Q

For web servers used for transmitting, processing or storing scoped data, are web server and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?

A

Yes, web server and application logs are relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access

Q

Is an API available to clients?

A

Yes, an API is available to clients

Q

Are mobile applications that access Scoped Systems and Data developed?

A

Yes, there are mobile applications developed that access Scoped Systems and Data

Q

For mobile applications that access scoped systems and data, are any actions performed by the application to access, process, transmit or locally store scoped systems and data?

A

Yes, actions are performed by the application to access, process, transmit or locally store scoped systems and data

Incident Event & Communications Management

Q

Is there an established Incident Management Program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?

A

Yes, our company has an established Incident Management Program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program

Q

Is there a formal incident response plan?

A

Yes, there is a formal incident response plan

Q

Does the incident response plan include escalation procedures?

A

Yes, the incident response plan includes escalation procedures

Q

Does the incident response plan include actions to be taken in the event of an information security event?

A

Yes, the incident response plan includes actions to be taken in the event of an information security event

Q

Are events on scoped systems or systems containing scoped data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?

A

Yes, events on scoped systems or systems containing scoped data relevant to supporting incident investigation are regularly reviewed using a specific methodology to uncover potential incidents

Q

Do events on scoped systems or systems containing scoped data relevant to supporting incident investigation include malware activity alerts such as uncleaned infections and suspicious activity?

A

Yes, events on scoped systems or systems containing scoped data relevant to supporting incident investigation include malware activity alerts such as uncleaned infections and suspicious activity

Business Resiliency

Q

Is there an established business resiliency program that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the program?

A

Yes, there is an established business resiliency program that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the program

Q

Does the business resiliency plan include a formal annual (or more frequent) executive management review of business continuity key performance indicators, accomplishments, and issues?

A

Yes, the business resiliency plan includes a formal annual (or more frequent) executive management review of business continuity key performance indicators, accomplishments, and issues

Q

Do the products and/or services specified in the scope of this assessment fall within the scope of the Business Resiliency program?

A

Yes, products and/or services specified in the scope of this assessment fall within the scope of the Business Resiliency program

Q

Are formal business continuity procedures developed and documented?

A

Yes, formal business continuity procedures are developed and documented

Q

Has senior management assigned the responsibility for the overall management of the response and recovery efforts?

A

Yes, senior management is assigned the responsibility for the overall management of the response and recovery efforts

Q

Is there a periodic (at least annual) review of your business resiliency procedures?

A

Yes, a periodic (at least annual) review of your business resiliency procedures is completed

Q

Are there any dependencies on critical third-party service providers?

A

Yes, there are dependencies on critical third-party service providers

Q

Do your critical third-party service providers have a communication plan in the event of a disruption that impacts the delivery of their products and services?

A

Yes, our critical third-party service providers have a communication plan in the event of a disruption that impacts the delivery of their products and services

Q

Is there a formal, documented exercise and testing program in place?

A

Yes, there is a formal, documented exercise and testing program in place

Q

Is there an annual schedule of planned business resiliency exercises and tests?

A

Yes, there is an annual schedule of planned business resiliency exercises and tests

Q

Are backups of scoped systems and data performed?

A

Yes, backups of scoped systems and data are performed

Q

Is there a policy or process for the backup of production data?

A

Yes, there is a policy or process for the backup of production data

Q

For backup of production data is backup media and restoration procedures tested at least annually?

A

Yes, backup media and restoration procedures are tested at least annually

Q

Are backup and replication errors reviewed and resolved as required?

A

Yes, backup and replication errors are required to be reviewed and resolved

Q

Is backup media stored offsite?

A

Yes, backup media is stored offsite

Q

Are backups containing scoped data stored in an environment where the security controls protecting them are commensurate with the production environment?

A

Yes, backups containing scoped data are stored in an environment where the security controls protecting them are commensurate with the production environment

Compliance

Q

Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements including intellectual property rights on business processes or information technology software products?

A

Yes, there are policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements including intellectual property rights on business processes or information technology software products

Q

Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues?

A

Yes, there is an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues

Q

Does the internal audit, risk management, or compliance department perform audits to ensure compliance with applicable legal, regulatory, or industry requirements?

A

Yes, the internal audit, risk management, or compliance department performs audits to ensure compliance with applicable legal, regulatory, or industry requirements

Q

Does the audit function have independence from the lines of business?

A

Yes, the audit function has an independence from the lines of business

Q

Are management reporting or reporting to government agencies maintained in accordance with applicable law?

A

Yes, management reporting or reporting to government agencies is maintained in accordance with applicable law

Q

Is a business license maintained in all jurisdictions where required?

A

Yes, a business license is maintained in all jurisdictions where required

Q

Are there mechanisms in place to notify affected clients for suspected or actual fraudulent activity?

A

Yes, there are mechanisms in place to notify affected clients for suspected or actual fraudulent activity

Q

Are marketing or selling activities conducted directly to client's customers?

A

Yes, marketing or selling activities are conducted directly to client's customers

Q

Is training conducted for Constituents with customer contact on consumer protection compliance responsibilities?

A

Yes, training is conducted for Constituents with customer contact on consumer protection compliance responsibilities

Q

Is there an incentive or compensation program for Constituents who directly sell/market to Client customers?

A

Yes, there is an incentive or compensation program for Constituents who directly sell/market to Client customers

Q

Are there documented policies and procedures to ensure compliance with applicable laws and regulations including Unfair, Deceptive, or Abusive Acts or Practices?

A

Yes, there are documented policies and procedures to ensure compliance with applicable laws and regulations including Unfair, Deceptive, or Abusive Acts or Practices

Q

Are there direct interactions with your client's customers?

A

No, there are no direct interactions with your client's customers

Q

Is a web site(s) maintained or hosted for the purpose of advertising, offering, managing, or servicing accounts, products or services to clients' customers?

A

Yes, a web site(s) is maintained or hosted for the purpose of advertising, offering, managing, or servicing accounts, products or services to clients' customers

Q

Are accounts opened, transactions initiated or other account maintenance activity (e.g., applying payments, receiving payments, transferring funds, etc.) through either electronic, telephonic, written or in-person requests made on behalf of your clients' customers?

A

Yes, there are accounts opened, transactions initiated or other account maintenance activity (e.g., applying payments, receiving payments, transferring funds, etc.) through either electronic, telephonic, written or in-person requests made on behalf of your clients' customers

Q

Are customer account activities monitored for unusual or suspicious activity?

A

Yes, customer account activities are monitored for unusual or suspicious activity

Q

Are electronic commerce web sites or applications used to transmit, process or store Scoped Systems and Data?

A

Yes, electronic commerce web sites or applications are used to transmit, process or store Scoped Systems and Data

Q

Are all transaction details i.e., payment card info and information about the parties conducting transactions, prohibited from being stored in the Internet facing DMZ?

A

Yes, all transaction details i.e., payment card info and information about the parties conducting transactions are prohibited from being stored in the Internet facing DMZ

Q

Are client audits and/or assessments permitted?

A

Yes, client audits and/or assessments are permitted

Q

Are artifacts available during a client assessment?

A

Yes, artifacts are available during a client assessment

Q

Are controls validated by independent, third party auditors or information security professionals?

A

Yes, controls are validated by independent, third party auditors or information security professionals

End User Device Security

Q

Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data?

A

Yes, End User Devices (Desktops, Laptops, Tablets, Smartphones) are used for transmitting, processing or storing Scoped Data

Q

For End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data, are security configuration standards documented?

A

Not Applicable

Q

For End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data, are activity alerts such as uncleaned infections and suspicious activity reviewed and actioned at least weekly?

A

No, activity alerts such as uncleaned infections and suspicious activity are not reviewed and actioned at least weekly

Q

For End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data, are defined procedures in place to identify and correct systems without anti-virus at least weekly?

A

No, defined procedures are not in place to identify and correct systems without anti-virus at least weekly

Q

For End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data, are constituents allowed to utilize mobile devices within your environment?

A

Yes, constituents are allowed to utilize mobile devices within your environment

Q

For constituents allowed to utilize mobile devices within your environment, is access to e-mail permitted?

A

Yes, access to e-mail is permitted

Q

For End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data, is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?

A

Yes, there is a mobile device management program in place that has been approved by management and communicated to appropriate constituents

Q

Are desktop computers used to transmit, process or store Scoped Systems and Data?

A

Yes, desktop computers are used to transmit, process or store Scoped Systems and Data

Q

For desktop computers used to transmit, process or store Scoped Systems and Data, are non-company managed PCs used to connect to the company network?

A

No, non-company managed PCs are not used to connect to the company network

Q

Are staff technically prevented from accessing the administrative environment via non-managed private devices?

A

Yes, staff are technically prevented from accessing the administrative environment via non-managed private devices

Network Security

Q

Are there external network connections (Internet, Extranet, etc.)?

A

Yes, there are external network connections (Internet, Extranet, etc.)

Q

For external network connections (Internet, Extranet, etc.), are there security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (Baseline configuration, patching, passwords, Access control)?

A

Yes, there are security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (Baseline configuration, patching, passwords, Access control)

Q

For external network connections (Internet, Extranet, etc.), is there an approval process prior to installing a network device?

A

Yes, there is an approval process prior to installing a network device

Q

For external network connections (Internet, Extranet, etc.), is every connection to an external network terminated at a firewall?

A

Yes, every connection to an external network is terminated at a firewall

Q

For external network connections (Internet, Extranet, etc.), do network devices deny all access by default?

A

Yes, network devices deny all access by default

Q

For external network connections (Internet, Extranet, etc.), do the firewalls have any rules that permit 'any' network, sub network, host, protocol or port on any of the firewalls (internal or external)?

A

No, firewalls do not have any rules that permit 'any' network, sub network, host, protocol or port on any of the firewalls (internal or external)

Q

For external network connections (Internet, Extranet, etc.), is remote access to administrative interfaces configured to require authentication and encryption?

A

Yes, remote access to administrative interfaces is configured to require authentication and encryption

Q

For external network connections (Internet, Extranet, etc.), are default passwords changed or disabled prior to placing the device into production?

A

Yes, the default passwords are changed or disabled prior to placing the device into production

Q

For external network connections (Internet, Extranet, etc.), is there a remote access policy for systems transmitting, processing and storing Scoped Systems and Data that has been approved by management and communicated to constituents?

A

Yes, there is a remote access policy for systems transmitting, processing and storing Scoped Systems and Data that has been approved by management and communicated to constituents

Q

For external network connections (Internet, Extranet, etc.), are encrypted communications required for all remote connections?

A

Yes, encrypted communications is required for all remote connections

Q

For external network connections (Internet, Extranet, etc.), are all available high-risk security patches applied and verified ?

A

Yes, all available high-risk security patches are applied and verified

Q

For external network connections (Internet, Extranet, etc.), is sufficient detail contained in logs to support incident investigation?

A

Yes, there is sufficient detail contained in logs to support incident investigation

Q

For external network connections (Internet, Extranet, etc.), are Network Intrusion Detection capabilities employed?

A

Yes, Network Intrusion Detection capabilities are employed

Q

For external network connections (Internet, Extranet, etc.), is there a DMZ environment within the network that transmits, processes or stores Scoped Systems and Data?

A

Yes, there is a DMZ environment within the network that transmits, processes or stores Scoped Systems and Data

Q

Are wireless networking devices connected to networks containing scoped systems and data?

A

Yes, there are wireless networking devices connected to networks containing scoped systems and data

Q

For wireless networking devices connected to networks containing scoped systems and data, is there a wireless policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?

A

Yes, there is a wireless policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy

Q

For wireless networking devices connected to networks containing scoped systems and data, are wireless connections secured with WPA2, and encrypted using AES or CCMP?

A

Yes, wireless connections are secured with WPA2, and encrypted using AES or CCMP

Q

Is remote terminal technology (e.g., RDP, Citrix) used to access Scoped Systems and Data remotely?

A

No, remote terminal technology (e.g., RDP, Citrix) is not used to access Scoped Systems and Data remotely

Privacy

Q

Is there access to, processing of, or retention of any client scoped Data that includes any classification of non-public personal information or personal data of individuals?

A

Yes, there is access to, processing of, or retention of any client scoped Data that includes any classification of non-public personal information or personal data of individuals

Q

Are transactions for Covered Accounts accessed, modified, or processed, including address changes and discrepancies?

A

Are transactions for Covered Accounts accessed, modified, or rocessed, including address changes and discrepancies?

Q

Are there documented policies and procedures for identifying and responding to relevant Red Flags on covered accounts, including address changes and discrepancies?

A

Yes, there are documented policies and procedures for identifying and responding to relevant Red Flags on covered accounts, including address changes and discrepancies

Q

Is there a documented identify theft prevention program approved by management in place to detect, prevent, and mitigate identify theft?

A

Yes, there is a documented identify theft prevention program approved by management in place to detect, prevent, and mitigate identify theft

Q

Is there a designated Data Protection Officer?

A

Yes, there is a designated Data Protection Officer

Q

Is there a process maintained to remove Personal Data based on the Right to be Forgotten if applicable to the services provided?

A

Yes, there is a process maintained to remove Personal Data based on the Right to be Forgotten if applicable to the services provided

Q

Are there privacy policies and procedures that are reviewed and revised at least annually?

A

Yes, there are privacy policies and procedures that are reviewed and revised at least annually

Q

Is there a management procedure maintained to monitor changes in applicable privacy regulations or contractual obligations?

A

Yes, there is a management procedure maintained to monitor changes in applicable privacy regulations or contractual obligations

Q

Is there a documented privacy policy or procedures maintained for the protection of information collected, transmitted, processed, or maintained on behalf of the client?

A

Yes, there is a documented privacy policy or procedures maintained for the protection of information collected, transmitted, processed, or maintained on behalf of the client

Q

Is there a formalized approval process to review and update data classification definitions and the documentation of data flows maintained and/or data inventories of client scoped privacy on a periodic basis?

A

Yes, there is a formalized approval process to review and update data classification definitions and the documentation of data flows maintained and/or data inventories of client scoped privacy on a periodic basis

Q

Are privacy risks identified and associated mitigation plans within a formally documented plan that is reviewed by management?

A

Yes, privacy risks identified and associated mitigation plans within a formally documented plan that is reviewed by management

Q

Are reasonable resources (e.g., time and money) allocated to mitigate identified privacy risks?

A

Yes, reasonable resources (e.g., time and money) are allocated to mitigate identified privacy risks

Q

Are procedures to assess privacy impact maintained and embed privacy requirements into new systems, applications or devices? (e.g., Privacy by Design)?

A

Yes, procedures are maintained to assess privacy impact and embed privacy requirements into new systems, applications or devices (e.g., Privacy by Design)

Q

Is privacy awareness training conducted for new employees at the time of onboarding?

A

Yes, there is privacy awareness training conducted for new employees at the time of onboarding

Q

Is privacy awareness training conducted on an annual basis?

A

Yes, privacy awareness training is conducted on an annual basis

Q

Is privacy awareness training extended to the organization's contractors or third parties?

A

Yes, privacy awareness training extended to the organization's contractors or third parties

Q

Is a process maintained to create and record of any detected or reported unauthorized disclosures of personal information?

A

Yes, a process is maintained to create and record of any detected or reported unauthorized disclosures of personal information

Q

Is there a process in place to monitor incident notification procedures to external authorities as required by applicable privacy or cyber security law?

A

Yes, there is a process in place to monitor incident notification procedures to external authorities as required by applicable privacy or cyber security law

Q

Is there a formal privacy incident communication procedure integrated with the information security incident response and escalation process?

A

Yes, there is a formal privacy incident communication procedure integrated with the information security incident response and escalation process

Q

Is notice provided about privacy policies and procedures related to client scoped data?

A

Yes, there is a notice provided about privacy policies and procedures related to client scoped data

Q

Does such notice identify the purposes for which personal information is collected, used, retained and disclosed?

A

Yes, there is a notice to identify the purposes for which personal information is collected, used, retained and disclosed

Q

Is a website privacy policy maintained that is developed, published, and communicated to all users that have access to client-scoped privacy data?

A

Yes, there is a website privacy policy maintained that is developed, published, and communicated to all users that have access to client-scoped privacy data

Q

Is there an ongoing process maintained to review and update privacy policies and notices on a periodic basis?

A

Yes, there is an ongoing process maintained to review and update privacy policies and notices on a periodic basis

Q

Is notice provided when information is directly collected from an individual?

A

Yes, there is a notice provided when information is directly collected from an individual

Q

Are notices communicated of privacy obligations to internal and external users?

A

Yes, there are notices communicated of privacy obligations to internal and external users

Q

Is there a documented privacy policies and procedures maintained that address choice and consent based on the legal, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data?

A

Yes, there is a documented privacy policies and procedures maintained that address choice and consent based on the legal, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data

Q

Where the use personal data requires explicit consent, are there mechanisms in place to obtain such consent prior to collection and consistent with the organization's privacy commitments or privacy policy?

A

Yes, where the use of personal data requires explicit consent, there are mechanisms in place to obtain such consent prior to collection and consistent with the organization's privacy commitments or privacy policy

Q

Are choices offered regarding the collection, use, retention, disclosure and disposal of client-scoped personal data communicated?

A

Yes, there are choices offered regarding the collection, use, retention, disclosure and disposal of client-scoped personal data communicated

Q

Is there a documented policy or procedure maintained that defines the basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information?

A

Yes, there is a documented policy or procedure maintained that defines the basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information

Q

For client-scoped Data, is data collected directly from an individual on behalf of the client?

A

Yes, for client-scoped Data, data is collected directly from an individual on behalf of the client

Q

Are there documented policies and operating procedures maintained regarding limiting the personal data collected and its use?

A

Yes, there are documented policies and operating procedures maintained regarding limiting the personal data collected and its use

Q

Are there documented privacy policies and procedures maintained that address data collection based on the legal, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data?

A

Yes, there are documented privacy policies and procedures maintained that address data collection based on the legal, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data

Q

Are there controls in place to ensure that the collection of personal information is limited?

A

Yes, there are controls in place to ensure that the collection of personal information is limited

Q

Are there controls in place to ensure that the collection and usage of personal information is limited and in compliance with applicable law?

A

Yes, there are controls in place to ensure that the collection and usage of personal information is limited and in compliance with applicable law

Q

Is there a policy or process for records retention to ensure that Personal Information is retained for no longer than necessary to fulfill the obligations or meet legal retention requirements?

A

Yes, there is a policy or process for records retention to ensure that Personal Information is retained for no longer than necessary to fulfill the obligations or meet legal retention requirements

Q

Is there a policy and process to limit any secondary use of client Scoped Data unless authorized?

A

Yes, there is a policy and process to limit any secondary use of client Scoped Data unless authorized

Q

Are there control mechanisms in place to mask, anonymize, or pseudonymous personal data to prevent loss, theft, misuse or unauthorized access?

A

Yes, there are control mechanisms in place to mask, anonymize, or pseudonymous personal data to prevent loss, theft, misuse or unauthorized access

Q

Is there a policy and/or process to limit or prevent the sharing of client-scoped Data with affiliates unless authorized?

A

Yes, there is a policy and/or process to limit or prevent the sharing of client-scoped Data with affiliates unless authorized

Q

Is client Scoped Data aggregated, appended, or modeled using outside data sources of personal information?

A

No, client Scoped Data is not aggregated, appended, or modeled using outside data sources of personal information

Q

If personal data is kept electronically or processed through automated means, are mechanisms in place to enable data portability for client scoped data?

A

Yes, where personal data is kept electronically or processed through automated means, mechanisms are in place to enable data portability for client scoped data

Q

If personal data of individuals is retained by your organization, are there processes and procedures to enable individuals to view, access, correct, amend, or delete inaccurate information?

A

Yes, where personal data of individuals is retained by your organization, there are processes and procedures to enable individuals to view, access, correct, amend, or delete inaccurate information

Q

Is there a documented process to reasonably authenticate the individual prior to fulfilling the individual's request for access to their personal information?

A

Yes, there is a documented process to reasonably authenticate the individual prior to fulfilling the individual's request for access to their personal information

Q

Is there a process to inform individuals in writing of the reason a request for access to their personal information was denied and the dispute mechanisms if any to challenge as specifically permitted or required by law or regulation?

A

Yes, there is a process to inform individuals in writing of the reason a request for access to their personal information was denied and the dispute mechanisms if any to challenge as specifically permitted or required by law or regulation

Q

Is client scoped data transmitted, processed, stored, disclosed to or retained by third parties?

A

Yes, there is client scoped data transmitted, processed, stored, disclosed to or retained by third parties

Q

Is client scoped data transmitted, processed, stored, disclosed to or retained by third parties?

A

Yes, there is client scoped data transmitted, processed, stored, disclosed to or retained by third parties

Q

Do agreements with third parties who have access or potential access to client scoped Data address confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of privacy data?

A

Yes, where there are agreements with third parties who have access, or potential access, to client scoped Data, confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of privacy data is addressed

Q

Is personal information accessed, disclosed, processed, transmitted or retained with third parties across national borders?

A

No, there is no personal information accessed, disclosed, processed, transmitted or retained with third parties across national borders

Q

Are there contractual controls established to ensure that personal information collected, transmitted, processed, stored or disclosed to or retained by third parties is limited to defined parameters for access, use and disclosure?

A

Yes, there are contractual controls established to ensure that personal information collected, transmitted, processed, stored or disclosed to or retained by third parties is limited to defined parameters for access, use and disclosure

Q

Are there documented policies, procedures or mechanisms to provide notice, and if required obtain consent for any new, changed usage of fourth parties, subcontractors, sub-processors, or sub-service organizations?

A

Yes, there are documented policies, procedures or mechanisms to provide notice, and if required obtain consent for any new, changed usage of fourth parties, subcontractors, sub-processors, or sub-service organizations

Q

Is there a documented data protection program with administrative, technical, and physical safeguards for the protection of client-scoped Data?

A

Yes, there is a documented data protection program with administrative, technical, and physical safeguards for the protection of client-scoped Data

Q

Are tests conducted of the effectiveness of the key administrative, technical, and physical safeguards for protecting personal information at least annually?

A

Yes, tests are conducted of the effectiveness of the key administrative, technical, and physical safeguards for protecting personal information at least annually

Q

Are mechanisms established so that access to personal information is limited to authorized personnel based upon their assigned roles and responsibilities?

A

Yes, mechanisms are established so that access to personal information is limited to authorized personnel based upon their assigned roles and responsibilities

Q

Is there a policy or procedures that provides notice to individuals of the administrative, technical, and physical safeguards taken to protection their personal data?

A

Yes, there is a policy or procedures that provides notice to individuals of the administrative, technical, and physical safeguards taken to protection their personal data

Q

For each software application hosted or operated by a third party that processes personal data, does the underlying contract identify the scope, nature, and purpose of processing, including the duration and types of personal data and categories of data?

A

Yes, for each software application hosted or operated by a third party that processes personal data, there is an underlying contract identifying the scope, nature, and purpose of processing, including the duration and types of personal data and categories of data

Q

Is there a process to maintain accurate and complete records of personal information based on its privacy commitments?

A

Yes, there is a process to maintain accurate and complete records of personal information based on its privacy commitments

Q

Is there a compliance risk management system maintained that address the quality and accuracy of personal information?

A

Yes, there is a compliance risk management system maintained that address the quality and accuracy of personal information

Q

Does the compliance risk management system address the quality of assembling and maintaining personal information?

A

Yes, the compliance risk management system addresses the quality of assembling and maintaining personal information.

Q

Is there a data protection function that maintains enforcement and monitoring procedures to address compliance for its privacy obligations for client-scoped privacy data?

A

Yes, there is a data protection function that maintains enforcement and monitoring procedures to address compliance for its privacy obligations for client-scoped privacy data

Q

Are there enforcement mechanisms in place to address privacy inquiries, complaints, disputes and recourse for violations of privacy compliance?

A

Yes, there are enforcement mechanisms in place to address privacy inquiries, complaints, disputes and recourse for violations of privacy compliance

Q

Are there policies and processes in place to log and report privacy complaints?

A

Yes, there are policies and processes in place to log and report privacy complaints

Q

Is an independent dispute mechanism maintained for resolution of privacy disputes?

A

Yes, there is an independent dispute mechanism maintained for resolution of privacy disputes

Q

Are applicable registrations, permits, approvals, or adequacy derogations maintained as required by Applicable Privacy Law?

A

Yes, there are applicable registrations, permits, approvals, or adequacy derogations maintained as required by Applicable Privacy Law

Threat Management

Q

Are Windows servers used as part of the Scoped Services?

A

Yes, Windows servers are used as part of the Scoped Services

Q

Is there an anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?

A

Yes, there is an anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy

Q

Does the anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy, include defined operating systems that require antivirus?

A

Yes, there are defined operating systems that require antivirus

Q

Does the anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy, include an interval between the availability of a new anti-malware signature update and its deployment no longer than 24 hours?

A

Not Applicable (Note: Update of Anti-virus signatures are dependent on the vendor/provider. Interval between updates are defined by the provider and our systems are updated immediately upon their posting)

Q

Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituent and an owner assigned to maintain and review the policy?

A

Yes, there is a vulnerability management policy or program that has been approved by management, communicated to appropriate constituent and an owner assigned to maintain and review the policy

Server Security

Q

Are Servers used for transmitting, processing or storing Scoped Data?

A

Yes, servers are used for transmitting, processing or storing Scoped Data

Q

For all Servers used for transmitting, processing or storing Scoped Data, are security configuration standards documented and based on external industry or vendor guidance?

A

Yes, security configuration standards are documented and based on external industry or vendor guidance

Q

For documented security configuration standards based on external industry or vendor guidance, are reviews performed regularly to validate compliance with documented standards?

A

Yes, reviews are performed regularly to validate compliance with documented standards

Q

Are all Servers used for transmitting, processing or storing Scoped Data configured according to security standards as part of the build process?

A

Yes, all servers are configured according to security standards as part of the build process

Q

For servers configured according to security standards as part of the build process, are all unnecessary/unused services uninstalled or disabled?

A

Yes, all unnecessary/unused services are uninstalled or disabled

Q

For servers configured according to security standards as part of the build process, are vendor default passwords removed, disabled or changed prior to placing the device or system into production?

A

Yes, vendor default passwords are removed, disabled or changed prior to placing the device or system into production

Q

For all Servers used for transmitting, processing or storing Scoped Data are all systems and applications patched regularly?

A

Yes, all systems and applications are patched regularly

Q

For all systems and applications patched regularly, are there any Operating System versions in use within the Scoped Services that no longer have patches released?

A

No, there are no Operating System versions in use within the Scoped Services that no longer have patches released

Q

For all Servers used for transmitting, processing or storing Scoped Data, is sufficient detail contained in Operating System and application logs to support security incident investigations (at a minimum, successful and failed login attempts, and changes to sensitive configuration settings and files)?

A

Yes, there is sufficient detail contained in Operating System and application logs to support security incident investigations (at a minimum, successful and failed login attempts, and changes to sensitive configuration settings and files)

Q

For all Servers used for transmitting, processing or storing Scoped Data, is Unix or Linux used as part of the Scoped Services?

A

Yes, Unix or Linux is used as part of the Scoped Services

Q

Where Unix or Linux servers are used as part of the Scoped Services, are users required to 'su' or 'sudo' into root?

A

Yes, users are required to 'su' or 'sudo' into root

Q

For all Servers used for transmitting, processing or storing Scoped Data are AS/400s used as part of the Scoped Services?

A

No, AS/400s are not used as part of the Scoped Services

Q

For all Servers used for transmitting, processing or storing Scoped Data, are Mainframes used as part of the Scoped Services?

A

No, mainframes are not used as part of the Scoped Services

Q

For all Servers used for transmitting, processing or storing Scoped Data are hypervisors used to manage systems used to transmit, process or store Scoped Data?

A

Yes, hypervisors are used to manage systems used to transmit, process or store Scoped Data

Q

For Hypervisors used to manage systems used to transmit, process or store Scoped Data, are Hypervisor hardening standards applied?

A

Yes, hypervisor hardening standards are applied

Q

For Hypervisors used to manage systems used to transmit, process or store Scoped Data, are there standard builds/security compliance checks?

A

Yes, there are standard builds/security compliance checks

Q

For Hypervisors used to manage systems used to transmit, process or store Scoped Data, are there current patches?

A

Yes, current patches

Q

For Hypervisors used to manage systems used to transmit, process or store Scoped Data, are unnecessary/unused services turned off?

A

Yes, unnecessary/unused services are turned off

Q

For Hypervisors used to manage systems used to transmit, process or store Scoped Data, is there sufficient information in the logs to evaluate incidents?

A

Yes, there is sufficient information in the logs to evaluate incidents

Q

For Hypervisors used to manage systems used to transmit, process or store Scoped Data, are passwords encrypted in transit?

A

Yes, passwords are encrypted in transit

Q

For Hypervisors used to manage systems used to transmit, process or store Scoped Data, are passwords encrypted or hashed in storage?

A

Yes, passwords are encrypted or hashed in storage

Q

For all Servers used for transmitting, processing or storing Scoped Data are Data Containers used to process or store Scoped Data?

A

No, data containers are not used to process or store Scoped Data

Cloud Hosting

Q

Are Cloud Hosting services (IaaS) provided?

A

No, Cloud Hosting services (IaaS) are not provided

Q

Is Cloud Hosting subcontracted?

A

No, Cloud Hosting is not subcontracted

Q

Is there a management approved process to ensure that backup image snapshots containing Scoped Data are authorized by Outsourcer prior to being snapped?

A

Not Applicable: We do not utilize cloud services for this application.

Q

Are default hardened base virtual images applied to virtualized operating systems?

A

Yes, default hardened base virtual images are applied to virtualized operating systems

Q

Does the Cloud Hosting Provider provide independent audit reports (e.g., Service Operational Control - SOC) for their cloud hosting services?

A

Not Applicable