Vendor Risk Management Policy

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

A. Scope

This policy shall only be enforced if for the requested service and/or in the required territory a Tier 1 service provider is not available or can for technology, business, commercial or other reasons not be selected.

B. Vendor Requirements

1. Has formal written Information Security Policies.
2. Will provide copies of the Information Security Policies.
3. Can provide results of a third-party external Information Security assessment conducted within the past 2 years (SAS-70, pen. test, vulnerability assess., etc.).
4. Maintains incident response procedures.
5. Has a policy to protect client information against unauthorised access; whether stored, printed, spoken or transmitted.
6. Has a policy that prohibits sharing of individual accounts and passwords.
7. Has a policy that implements the following Information Security concepts: need to know, least privilege and checks and balances.
8. Requires employees to be educated and qualified.
9. Implements AAA (Authentication, Authorisation, Accounting) for all users.
10. Performs background checks for individuals handling confidential information.
11. Has termination or job transfer procedures that immediately protect unauthorised access to information.
12. Provides customer support with escalation procedures.
13. Has documented change control processes.
14. Requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements.
15. Has a policy that implements federal and provincial regulatory requirements.
16. Maintains a routine user Information Security awareness program.
17. Has a formal routine Information Security risk management program for risk assessments and risk management.

1. Architecture Requirements

1. Will provide a network topology diagram/design.
2. Implements network firewall protection.
3. Implements web application firewall protection.
4. Implements host firewall protection.
5. Maintains routers and ACLs.
6. Provides network redundancy.
7. Has IDS/IPS technology implemented.
8. Uses DMZ architecture for Internet systems.
9. Adheres to the practice that web applications, which 'face' the Internet, are on a server different from the one that contains the database.
10. Uses enterprise virus protection on all systems.
11. Follows a program of enterprise patch management.
12. Ensures that remote access is only possible over secure connections.
13. Uses separate physical and logical development, test and production environments and databases.

14. Secures development and test environments using, at a minimum, equivalent security controls as the production environment.
15. Has managed, secure access points on its wireless network.

2. Configuration Requirements

1. Implements encryption for confidential information being transmitted on external or Internet connections with a strength of at least AES 256 bit or uses TLS 1.2
2. Implements encryption for confidential information at rest with a strength of at least AES 256 bit.
3. Has password-protected screen savers that activate automatically to prevent unauthorised access when idle, for computers used by system's support users.
4. Removes all unnecessary services from computers.
5. Changes or disables all vendor-supplied default passwords or similar “published” access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products.
6. Uses passwords that are a min. of 8 characters, expire at least annually & have complexity requirements.
7. Ensures that passwords are never stored in clear text or are easily decipherable.
8. Checks all systems and software to determine whether appropriate security settings are enabled.
9. Manages file and directory permissions following least privilege and need-to-know practices.
10. Implements redundancy or high availability for critical functions.
11. Authenticates all user access with either a password, token or biometrics.
12. Formally approves, tests and logs all system changes.
13. Does not use production data for both development and testing.
14. Uses artificial data in both development and test environments.
15. Limits access to development and test environments to personnel with a need to know.
16. Sets the account lockout feature for successive failed logon attempts on all system's support computers.

3. Product Design Requirements

1. Ensures that if the product integrates with portable devices, confidential information is encrypted when stored on these portable devices and requires password access.
2. Ensures that access to confidential information, across a public connection, is encrypted with a secured connection and requires user authentication.
3. Implements protections for CVEs in a timely manner to protect from exploits.
4. Audits the application against the OWASP Top 10 Application Security Risks.
5. Ensures that application server and database software technologies are kept up-to-date with the latest security patches.
6. Uses threat modeling in their software development lifecycle (SDL).
7. Performs security code reviews as part of their SDL.

4. Access Control Requirements

1. Immediately removes, or modifies access, when personnel terminate, transfer, or change job functions.
2. Achieves individual accountability by assigning unique IDs and prohibiting password sharing.
3. Ensures that critical data, or systems, are accessible by at least two trusted and authorised individuals, in order to limit having a single point of service failure.
4. Ensures that users have the authority to only read or modify those programs, or data, which are needed to perform their duties.

5. Monitoring Requirements

1. Reviews access permissions monthly for all server files, databases, application, etc.
2. Implements system event logging on all servers and records at a minimum who, what, and when for all transactions.
3. Reviews and analyses after hours system accesses, at least monthly.
4. Reviews system logs for failed logins, or failed access attempts monthly.
5. Reviews and removes dormant accounts on systems at least monthly.
6. Reviews web server logs weekly for possible intrusion attempts and daily for significant changes in log file size as an indicator of compromise.
7. Reviews network and firewall logs at least monthly.
8. Reviews wireless access logs at least monthly.
9. Performs scanning for rogue access points at least quarterly.
10. Performs vulnerability scanning at least quarterly.
11. Performs penetration testing at least anually.
12. Checks routinely that password complexity is adhered to.

6. Physical Security Requirements

1. Controls access to secure areas. E.g. key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.
2. Controls access to server rooms and follows least privilege and need-to-know practices for those facilities.
3. Has special safeguards in place for computer rooms. e.g. cipher locks, restricted access, room access log, card swipe access control, etc.
4. Shreds or incinerates printed confidential information.
5. Prohibits or encrypts confidential information on laptops & mobile devices.
6. Positions desktops, which display confidential information, in order to protect from unauthorised viewing.
7. Escorts all visitors in computer rooms or server areas.
8. Implements appropriate environmental controls, where possible, to manage equipment risks. E.g. fire safety, temperature, humidity, battery backup, etc.
9. Has no external signage indicating the content or value of the server room or any room containing confidential customer information.

10. Provides an export copy of all of the customer's data in a mutually agreed upon format at the end of the contract.
11. Follows forensically secure data destruction processes for confidential data on hard drives, tapes & removable media when it's no longer needed and at the end of the contract term.

7. Contingency Requirements

1. Has a written contingency plan for mission critical computing operations.
2. Has emergency procedures and responsibilities documented and stored securely at multiple sites.
3. Reviews and updates the contingency plan at least annually.
4. Has identified computing services that must be provided within specified critical timeframes, in case of a disaster.
5. Has identified cross-functional dependencies, so as to determine how the failure in one system may negatively impact another one.
6. Has written backup procedures and processes.
7. Tests the integrity of backup media quarterly.
8. Stores backup media in a secure manner and controls access.
9. Maintains a documented and tested disaster recovery plan.
10. Uses off-site storage and has documented retrieval procedures for backups.
11. Password protects and encrypts all backups.
12. Provides rapid access to backup data.

8. Business Associate Requirements

1. Confidentiality agreements have been signed before proprietary and/or confidential information is disclosed to the vendor's business associates.
2. Vendor's business associate contracts, or agreements, are in place and contain appropriate risk coverage for customer requirements.
3. Vendor's business associates are aware of customer security policies and what is required of them.
4. Vendor's business associate agreements document the agreed transfer of customer's data when the relationship terminates.