WedgeBPM

WedgeBPM's Client Data Safeguards

The following terms describe the technical and organizational measures, internal controls and information security routines that WedgeBPM maintains to safeguard data provided by or on behalf of our clients in connection with a client service engagement ("Client Data").

These security measures are intended to protect Client Data when in WedgeBPM's environments (e.g., systems, networks, facilities) against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. When Client Data includes personal data, our implementation of and compliance with these measures (and any additional security measures set out in the applicable client agreement) is designed to provide an appropriate level of security in respect of the processing of the personal data. WedgeBPM may change these measures from time to time, without notice, so long as any such revisions do not materially reduce or degrade the protection provided for the Client Data.

STANDARD DATA SAFEGUARDS:

1. Organization of Information Security
   a. Security Ownership. WedgeBPM will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.
   b. Security Roles and Responsibilities. WedgeBPM's personnel with access to Client Data will be subject to confidentiality obligations.
   c. Risk Management Program. WedgeBPM will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Client Data in connection with the applicable agreement between the Parties.

2. Asset Management
   a. Asset Inventory. WedgeBPM will maintain an asset inventory of its infrastructure, network, applications and cloud environments. WedgeBPM will also maintain an inventory of its media on which Client Data is stored. Access to the inventories of such media will be restricted to personnel authorized in writing to have such access.
   b. Data Handling. WedgeBPM will
      1. Classify Client Data to help identify such data and to allow for access to it to be appropriately restricted.
      2. Limit printing of Client Data from its systems to what is minimally necessary to perform services and have

procedures for disposing of printed materials that contain Client Data.

3. Require its personnel to obtain appropriate authorization prior to storing Client Data outside of contractually approved locations and systems, remotely accessing Client Data, or processing Client Data outside the Parties' facilities.

3. Communications and Operations Management

a. Operational Policy. WedgeBPM will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Client Data.

b. Mobile Device Management (MDM)/Mobile Application Management (MAM). WedgeBPM will maintain a policy for its mobile devices that:

1. Enforces device encryption.
2. Prohibit use of blacklisted apps.
3. Prohibits enrollment of mobile devices that have been "jail broken."

c. Data Recovery Procedures. WedgeBPM will

1. Have specific data recovery procedures with respect to its systems in place designed to enable the recovery of Client Data being maintained in its systems.
2. Review its data recovery procedures at least annually.
3. Log data restoration efforts with respect to its systems, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

d. Malicious Software. WedgeBPM will have anti-malware controls to help avoid malicious software gaining unauthorized access to Client Data, including malicious software originating from public networks.

e. Data Beyond Boundaries. WedgeBPM will

1. Encrypt Client Data that it transmits over public networks.
2. Protect Client Data in media leaving its facilities (e.g., through encryption).
3. Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems.

f. Event Logging.

1. For its systems containing Client Data, WedgeBPM will log events consistent with its stated policies or standards.

4. Access Control

a. Access Policy. WedgeBPM will maintain a record of security privileges of individuals having access to Client Data via its systems.

b. Access Authorization. WedgeBPM will

   1. Maintain and update a record of personnel authorized to access Client Data via its systems.
   2. When responsible for access provisioning, promptly provision authentication credentials.
   3. Deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed 90 days).
   4. Deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days.
   5. Identify those personnel who may grant, alter or cancel authorized access to data and resources.
   6. Ensure that where more than one individual has access to its systems containing Client Data, the individuals have unique identifiers/log-ins (i.e., no shared ids).

c. Least Privilege. WedgeBPM will

   1. Only permit its technical support personnel to have access to Client Data when needed
   2. Maintain controls that enable emergency access to productions systems via firefighter ids, temporary ids or ids managed by a Privileged Access Management (PAM) solution.
   3. Restrict access to Client Data in its systems to only those individuals who require such access to perform their job function.
   4. Limit access to Client Data in its systems to only that data minimally necessary to perform the services.
   5. Support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., developer/ reviewer, developer/tester).

d. Integrity and Confidentiality. WedgeBPM will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.

e. Authentication. WedgeBPM will

   1. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems.
   2. Where authentication mechanisms are based on passwords, require that the passwords are renewed regularly.
   3. Where authentication mechanisms are based on passwords, require the password to contain at least eight characters and three of the following four types of characters: numeric (0-9), lowercase (a-z), uppercase (A-Z), special (e.g., !, *, C, etc.).
   4. Ensure that de-activated or expired identifiers are not granted to other individuals.
   5. Monitor repeated attempts to gain access to its information systems using an invalid password.
   6. Maintain industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.
   7. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.

e. Multi Factor Authentication. WedgeBPM will implement Multi- Factor Authentication for internal access and remote access over virtual private network (VPN) to its systems.

5. Penetration Testing and Vulnerability Scanning of WedgeBPM Systems.

a. At least annually, WedgeBPM will perform penetration and vulnerability assessments on WedgeBPM's IT environments in accordance with WedgeBPM's internal security policies and standard practices.

b. WedgeBPM agrees to share with Client summary level information related to such tests as conducted by WedgeBPM to the extent applicable to the Services.

c. For clarity, as it relates to such penetration and vulnerability testing, Client will not be entitled to (i) data or information of other customers or clients of WedgeBPM; (ii) test third party IT environments except to the extent WedgeBPM has the right to allow such testing; (iii) any access to or testing of shared service infrastructure or environments, or (iv) any other Confidential Information of WedgeBPM that is not directly relevant to such tests and the Services.

d. For any WedgeBPM IT systems that are physically dedicated to Client, the Parties may agree to separate, written testing plans and such testing will not to exceed two tests per year.

6. Network and Application Design and Management. WedgeBPM will

a. Have controls to avoid individuals gaining unauthorized access to Client Data in its systems.

b. Use email-based data loss prevention to monitor or restrict movement of sensitive data.

c. Use network-based web filtering to prevent access to unauthorized sites.

d. Use firefighter IDs or temporary user IDs for production access.

e. Use network intrusion detection and / or prevention in its systems.

f. Use secure coding standards.

g. Scan for and remediate OWASP vulnerabilities in its systems.

h. To the extent technically possible, expect that the Parties will work together to limit the ability of WedgeBPM personnel to access non-Client and non-WedgeBPM environments from the Client systems.

i. Maintain up to date server, network, infrastructure, application and cloud security configuration standards.

j. Scan its environments to ensure identified configuration vulnerabilities have been remediated.

7. Patch Management

a. WedgeBPM will have a patch management procedure that deploys security patches for its systems used to process Client Data that includes