SalesforLife | **Data Security FAQ**

QUESTION	RESPONSE	COMMENTS
HUMAN RESOURCES SECURITY (HRS)		
Is there an acceptable use policy and/or contractual agreement in place with employees, contractors and/or third-party staff documenting cybersecurity responsibilities?	YES	Every employee and/or contractor has an official agreement where data, privacy and security are paramount.
Does each system (business applications, computer systems and networks) have a designated business owner that has accepted responsibility to protect it?	YES	Product and Operations manage all systems and are responsible for privacy, data and overall security.
Do you perform pre-employment background checks on all employees?	YES	This is part of our recruiting process for all employees/contractors.
CYBERSECURITY EDUCATION & AWARENESS (CEA)		
Do you have a security awareness program in place, including annual training?	YES	All employees/contractors attend annual training on data, privacy and security.
INFORMATION RISK ANALYSIS (RSK)		
Do you have an information security risk assessment program?	YES	Product & Operations is responsible for this and there are protocols in place for security risk.
ASSET MANAGEMENT (AST)		
Have you implemented an enterprise-wide security data classification policy resulting in appropriate security controls to protect sensitive data?	YES	Supported by Executive oversight.
Do you have a documented asset management system in place that tracks hardware, software, and licensing?	YES	Yes. We use an in-house built tracking system.
Do you have procedures in place to ensure the security of your supply chain?	N/A	We are a data-centric and virtual cloud business where no physical products are exchanged, sold or traded.
IDENTITY AND ACCESS MANAGEMENT (IAM)		
Is there a policy to implement role-based access control in accordance with the principle of least privilege?	YES	We provide role based access to employees, not everyone has access to everything.
Do you have a documented account management process to ensure users have authorization prior to being granted system access; access privileges are reviewed at least every six (6) months; access is revoked upon a user's change in role; and access is revoked immediately upon termination?	YES	A documented process is in place and managed by our Product & Operations teams with Executive oversight.
Do you have a policy that requires an individual identifier per user (not shared or group identifiers)?	YES	Yes, we have this policy in place.
Do you require strong authentication mechanisms (i.e. strong passwords, smart cards, or biometric devices)?	YES	All of our systems, platforms and apps require this.
Do you have a policy that requires privileged accounts be separate from a normal, non-privileged user account?	YES	Information access to our app is determined with privileges.
Do you have a policy that requires multi-factor authentication for privileged access?	YES	Yes, the app requires 2-Factor Authentication for every user
SYSTEM CONFIGURATION (SC)		
Are host systems (operating system, database, applications, etc.) configured based on industry standards?	YES	Yes, supported by industry leading platforms.
SYSTEM MONITORING (SM)		
Do you have a policy that requires logging key-security events?	YES	Yes we have. This is managed by our Product & Operations team.
Do you have a policy that requires the review of log alerts and security events on a regular basis?	YES	Yes we have. This is managed by our Product & Operations team.
Do you monitor your network for malicious activity?	YES	Our systems, platforms and apps use known commercial providers (such as Google, Zoom, Zoho and more) and as such, these cloud providers are monitoring.
NETWORK SECURITY (NET)		
Do you utilize defense-in-depth principles in your network architecture to prevent unauthorized access?	N/A	All systems are in the cloud from leading commercial providers (such as Google, Zoom, Zoho, etc.) and access is only available to privileged users within our internal team and a customer's team.
Do you ensure that all access points are secured and exist only if specifically required for business functionality?	YES	All systems are in the cloud from leading commercial providers (such as Google, Zoom, Zoho, etc.) and access is only available to privileged users within our internal team and a customer's team.
Is wireless access to your internal network(s) authorized, authenticated, and encrypted?	N/A	Not applicable.
Do you implement technical measures to detect and mitigate distributed denial-of-service (DDoS) attacks?	YES	We've implemented process to prevent DDoS and manage its effects. Additionally, our cloud partners have policies of this nature also (Google, Zoho, Zoom, Digital Ocean, etc.)
CRYPTOGRAPHY (CRY)		
Do you have documented standards and procedures to manage cryptographic keys and ensure protection against unauthorized access, destruction, or compromise through loss, corruption, or disclosure?	N/A	Not applicable. All content is in the cloud.
Do you have a document policy requiring sensitive information/PII to be encrypted in transit and at rest on all devices?	N/A	Not applicable. All content is in the cloud.
MALWARE PROTECTION (MAL)		
Do you have enterprise-wide capabilities for detection, prevention, and recovery related to malware attacks or infections?	YES	Our cloud partners have this policy (Google, Zoho, Zoom, Digital Ocean, etc.).
Do you have malware detection and repair software installed and configured to scan all systems on a regular basis?	YES	Our cloud partners have this policy (Google, Zoho, Zoom, Digital Ocean, etc.).
VULNERABILITY MANAGEMENT (VM)		
Do you have a vulnerability management program that includes: vulnerability identity and remediation, software and firmware patching, and hardware maintenance?	YES	Our cloud partners have this policy (Google, Zoho, Zoom, Digital Ocean, etc.).
Do you scan all internet-facing websites for security vulnerabilities on at least an annual basis or after changes have been made?	YES	Our cloud partners have this policy (Google, Zoho, Zoom, Digital Ocean, etc.).
COMMUNICATIONS & OPERATIONS MANAGEMENT (COMM)		
Do you provide security training to all system administrators?	YES	Our Product & Operations teams undergo security, data and privacy training.
Do you have policies in place to ensure separation of duties?	YES	Product and Operations conduct different duties with regard to security, data and privacy.
SYSTEM ACQUISTION, DEVELOPMENT & MAINTENANCE (DEV)		
Do you appropriately test during development to ensure proper security controls?	YES	Our software developers build with security in mind.
Do you have a policy restricting production data being used in a non-production environment?	YES	Our software developers use staging servers for all testing.
Do you have a documented software development lifecycle management process that includes industry-recognized leading practices (OWASP)?	YES	We use best-in-class process for all software development.
Do you have a documented procedure for secure sanitization of media?	YES	Via a quarterly media/content audit, we augment consistently.
Do you maintain a lifecycle process for all software?	YES	Yes we follow a complete software cycle.
CHANGE MANAGEMENT (CFG)		
Do you have a documented change control process in place for all production systems?	YES	Yes, we maintain all records.
Do you maintain your change control records?	YES	Yes, we maintain this.
CYBERSECURITY INCIDENT MANAGEMENT (IM)		
Do you document all cybersecurity incidents and maintain a documented cybersecurity event management process that covers the incident response, escalation, and remediation of cybersecurity events and incidents?	YES	Our cloud partners (Google, Zoho, Zoom, Digital Ocean, etc.) all do this by default and we also conduct this process with our app.
Is there a process to notify your customer without delay about any cybersecurity incident that could have an impact on your customer's business operations?	YES	We notify immediately for any cybersecurity event that can impact our customers.
Do you have processes for managing incidents that require forensic investigation and ensure preservation of evidence and proper chain of custody?	YES	Our cloud partners (Google, Zoho, Zoom, Digital Ocean, etc.) all do this by default and we also conduct this process with our app.
BUSINESS CONTINUITY & DISASTER RECOVERY (BCDR)		
Do you have a Business Continuity and Disaster Recovery (BCDR) plan?	YES	In the event of our app or systems going down, business can still be conducted regularly and manually.
Do you perfom tests of your BCDR plan?	N/A	Not applicable.
Are your applications, systems, and networks run on robust, reliable hardware and software supported by appropriate backup hardware and facilities where necessary?	YES	We are completely in the cloud and use leading commercial providers' infrastructure (Google, Zoom, Zoho, Digital Ocean, etc.).
Are backups of essential information and software performed on a regular basis?	YES	We have a process for this.
PROCESSING FACILITIES (PRC)		
Do you have processes in place to notify your customer before relocating any physical storage location of customer data to a country different from the one(s) documented in the current statement of work or contract?	N/A	Not applicable.
VENDOR MANAGEMENT (VND)		
Do you have a formal process to address due care and due diligence considerations (to include assessing and monitoring of the security stance) in the selection and management of downstream third-party vendors?	YES	All third-party vendors are chosen with care and compliance with our security, data & privacy requirements.
Is a documented termination of service process in place with all third-party vendors to ensure the recovery and removal of customer data?	YES	This is in place.
Do you address indemnification considerations with third-party vendors that could have an impact on your customer business operations with vendor?	YES	This is in place.
Do you have non-disclosure agreements with all external parties?	YES	This is in place.
Do you execute a Data Processing Agreement (DPA) with a third-party if you process, store, or transmit any data related to residents of the European Economic Area?	YES	All third-party vendors are chosen with care and compliance with our security, data & privacy requirements.
Do you have a process in place to notify your customer of a change in third-party vendor when your customer data is impacted?	YES	This process exists and is in place.
COMPLIANCE (CMP)		
Do you have a policy requiring compliance with applicable statutory, regulatory, and contractual requirements (i.e. PCI-DSS, HIPAA, SOX, GDPR, etc.)?	YES	Our cloud-based partners are leading commercial providers and have this policy in place.
Do you maintain a process to document non-compliance with any statutory, regulatory, or contractual requirements?	YES	Our cloud-based partners are leading commercial providers and have this policy in place.
Do you have a breach notification process that meets all applicable legal and contractual requirements?	YES	We notify customers of breaches and any business impact it may bave.
Do you have processes in place to notify customers when there are requests for access, to cease or not begin processing, to rectify, block, erase or destroy any personal data received?	YES	Yes. Requests can be made any time to dataprivacy@salesforlife.com.
Do you have policy that limits the collection of personal information from individuals to the minimum necessary to achieve your business goals?	YES	Only minimal information is collected to achieve the business outcomes.