Vendor Software Security Checklist

Security and Privacy by Design

Third-party software applications, including web applications and mobile applications, have become an integrated part of information systems that individuals, businesses, and organizations rely on. We often entrust software applications with **confidential** and **proprietary information**.

**Security and privacy features and controls** are important to:

* Protect the integrity of our data.
* Prevent data loss.
* Manage the risks of unauthorized access to or disclosure of our data.
* Help meet privacy laws and regulations.

This checklist helps you perform a **preliminary security review** of a software application as part of your vendor assessment to help you make informed decisions.

|  |  |  |
| --- | --- | --- |
| **1.** | **Account Management** | **Notes** |
|  | **User Provisioning/Deprovisioning**  Can user accounts be activated, updated, and deactivated manually by administrators or automatically through APIs? |  |
|  | **Automated Functions**  What automation is available to help you manage user accounts? Please consider:   * Reporting of active user accounts, including levels of access * Deactivation of inactive accounts * Notifications for account changes * Notifications for high-risk user policy changes (i.e., high levels of access granted). * Inactivity logout |  |
|  | **Audit Logs**  Can the software help you track critical actions performed by users, including those with administrative access?   * Critical end user activities, such as record uploads, training completions, and form submissions.      * Administrative updates to user accounts, such as adding or deleting personal information. |  |
| **2.** | **Access Control** |  |
|  | **Separation of Duties**  Can you grant user access to data and areas of the system based on users’ job roles and responsibilities in line with the standard of least privilege? |  |
|  | **Restricted Public Access**  Does the system allow you to control which information or content is publicly available (i.e., accessible to individuals without them logging in)? |  |
|  | **Data Classification and Restrictions**  Does the system allow you to apply global access controls to certain types of information, specific information fields (such as personally identifiable information), documents, and forms?  Does the system allow you to customize how certain types of information, specific information fields, documents, and forms are made available to end users and administrators? |  |
| **3.** | **Login Authentication** |  |
|  | **Password Standards**  Can you enforce password requirements, such as upper and lower-case letters, numbers, and characters?  Consider software systems that allow or prevent trust devices, require regular password updates, or prevent use of previously used passwords. |  |
|  | **Multifactor Authentication**  Does the software allow you to turn on and strategically apply multifactor authentication (MFA) requirements to your users? |  |
|  | **Single Sign-on (SSO)/Security Assertion Markup Language (SAML)**  Will your users be able to access their accounts through one set of login credentials, such as their Microsoft account login? |  |
|  | **Unsuccessful Login Attempts**  Does the software enforce a limit on invalid login attempts and implement a mechanism, to secure the account from unauthorized access and automated attacks.  E.g., , Prompting an additional secret question, locking the account for a specific time period, or requiring a reCAPTCHA. |  |
| **4.** | **Data Security and Integrity** |  |
|  | **Encryption**  Is data encrypted at rest and in transit following industry standards, such as transport layer security (TLS 1.2 or 1.3)?  Are data encryption standards, such as AES 256, applied to highly sensitive user data, such as passwords and personally identifiable information? |  |
|  | **Boundary Protection**  Does the software system establish physical or logical boundaries (managed interfaces) between publicly accessible components and private components?  Have boundary protection devices been implemented at these interfaces, such as firewalls, gateways, and routers, which restrict access and transfer of information? |  |
|  | **Security Filters**  Are security filters applied to data structures to check information added by users or uploads made by users? For example, file types, file sizes, data value ranges, and hidden content.  Does the software have features that can restrict the transfer of information based on IP addresses? |  |
|  | **Segregation of Data (Multi-tenant SaaS Environments)**  Is client data physical or logical segregated such that users in one client cannot access the data of another client? |  |
|  | **Monitoring**  Does the vendor apply tools, including anti-malware, to continuously monitor the application for system health, abnormal activity, and general performance?  Are there intrusion detection and prevention mechanisms configured in the application, including web application firewalls? |  |
|  | **API Management**  Request the vendor’s API documentation to check their API authentication requirements, rate limits, whitelisted IPs, and key management practices. |  |
|  | **Vulnerability Management**  Does the vendor perform independent tests regularly to identify vulnerabilities (e.g., penetration tests and vulnerability scans)?  Is there a process in place to assess and resolve identified vulnerabilities? |  |
|  | **Datacentre Security**  Where is the data physically stored?  Is the data stored in a location with robust physical security controls that meet industry standards, such as SSAE standards? |  |
|  | **Patch Management**  Does the vendor implement critical security patches in a timely manner? |  |
|  | **Redundancy**  Are there systems to protect data from accidental destruction or loss that include frequent backups (e.g., hourly, daily, etc.)?  Are backups verified and maintained for a sufficient amount of time, so data can be recovered?  Is the software designed to avoid single point of failures of critical system architectural components? |  |
| **5.** | **Service Level Commitment** |  |
|  | **Communications**  Are clients and users notified appropriately of planned system outages, software updates, and issues? |  |
|  | **Reporting and Resolution**  Does the vendor have a process for clients and users to report bugs, vulnerabilities, and potential security incidents?  Does the vendor have a published commitment describing response and remediation times related to issues reported by clients and users? |  |
|  | **Testing and Validation**  Does the vendor provide you with a demo application environment to view and test the software functionality and security features prior to commitment of use?  Can software users participate in beta testing of updates, participate in feature updates, and verify bug fixes? |  |
|  | **Customer Support**  Is there easily accessible and published contact information for all users to request help regarding their personal accounts, performing advanced configuration tasks, and highly technical issues?  Does the Support team respond quickly to a variety of different communication channels? |  |
| **6.** | **Security Program** |  |
|  | **Recognized Security Standards**  Does the vendor meet or comply with any internationally-recognized industry standards, such as SOC 2, PCI DSS, and ISO-27001? |  |
|  | **Security Framework**  Does the vendor have a global security standard that defines and sets a security framework for the entire infrastructure of the software? |  |
|  | **Risk Management**  Does the vendor have a risk management program to identify and eliminate or mitigate new and evolving risks, which includes the use of contractors to provide software services? |  |
|  | **Endpoint Security**  Does the vendor apply security controls and standards for the devices that their employees use to access the software system and client data?  Does the vendor have data sanitization processes for ensuring data on their devices are securely removed or destroyed? |  |
|  | **Policies, Standards, and Procedures**  Does the vendor have policies that govern access to the software architecture, servers, databases, and security controls (e.g., firewalls), including policies that govern access to client and user data? Policies may include access by VPN, MFA, and a strict user role provisioning process for write and root access based on standards of least privilege.  Does the vendor have secure coding standards that follows industry best practices, such as OWASP Top 10?  Does the vendor apply a change management process to ensure software updates avoid causing you interruptions and introducing software vulnerabilities?  Does the vendor have an employee management program with hiring practices that include confidentiality and intellectual property agreements, privacy training, skill assessments, and reference checks? Do offboarding procedures include timely revocation of access to the software and client data? |  |
|  | **Security Training**  Does the vendor ensure its team is properly trained in cyber security on an ongoing basis? |  |
|  | **Security Incident Response**  Does the vendor have a process to respond quickly and effectively to potential and actual data breaches and security threats?  Does this response include notification of affected parties? |  |
|  | **Business Continuity and Disaster Recovery**  What controls are in place to ensure continuous software uptime with minimal outages?  Does the vendor have a disaster recovery plan that is tested annually through a simulation or tabletop exercise? |  |
|  | **Insurance**  Does the vendor have general liability insurance that includes cyber risk insurance? |  |
| **7.** | **Privacy** |  |
|  | **Privacy Policy**  Does the vendor have a publicly available privacy policy that acknowledges privacy laws and regulations relevant to you?  Does their privacy policy make clear how information is collected, used, shared, and stored? |  |
|  | **Individual Access to Personal Information**  Does the vendor have a process that allows end users to review, request, update, and delete their personal information stored within the software? |  |
|  | **Confidentiality Agreement**  Does the vendor agree to your company’s confidentiality agreement? |  |

Data security and privacy is a growing priority for individuals and organizations. We believe in security by design wherever possible, while providing our clients flexibility in managing their security and privacy controls.

If you have any questions, do not hesitate to contact us at sales@bistraining.ca