



Minimum Security Specification.

Vendor quality standards for client hosted software platforms.

Platforms

Any client hosted system must support running in Microsoft Azure and on one of the following platforms (as a minimum):

- Windows server 2019
- Debian 11
- Ubuntu 20.04
- CentOS 7

Database

- Any installation that requires access to a database that runs on a different server must be able to run effectively on networking with a typical latency of no more than 2ms.
- Any database technology will be considered but MS SQL is preferred. The vendor will need to manage and maintain the backup process for any database that is not Microsoft SQL.

UI

- Access to the UI must be done through a modern web browser, our preference would be Microsoft edge in native mode not IE compatibility mode.
- Access to the UI must be done via the browser over HTTPS and not utilise any non-standard ports.
- Our preference would be that any UI uses native technologies in the browser and not employ any extensions or plug ins except where it enhances the security of the access.

Mobile Access

If the mobile application requires access to hosted systems it must be able to be routed via Azure web application firewall. Any exemptions on common threat vectors must be clearly defined and made clear prior to submission.

Security

We expect our software vendors to adhere to quality standards throughout the supported life of their products or until the customer (Adra) terminates any agreement. The following list is given as a minimum best practice that the customer (Adra) expects to be adhered to, the list is expected to be incorporated into the final agreed service level agreement between the vendor and the customer or added as an addendum to any service level agreement.

The following standards apply to vendors hosting their platform on infrastructural equipment owned and hosted by the customer.

We request that they (the vendor) comply with at least one of the following recognised industry security standards: ISO/IEC 27001, NIST frameworks, or the CIS Controls.

Vendors should conduct quarterly vulnerability assessments and scans to identify potential security weaknesses in their software and infrastructure. If the vendors software requires an update, scans should be done after installation and prior to releasing the update to the production environment. This information should be shared with the customer either electronically or during account meetings.

The vendor must be capable of demonstrating a clear process for timely patch management, including the monitoring of vulnerabilities, assessment of risks, and the prompt deployment of patches. Adra would expect the vendor to prioritise patches based on the CVSS score and patch or mitigate critical vulnerabilities as soon as they become aware. The vendor will be expected to have a patch criticality matrix or equivalent available for the customer to review.

The vendor is required to perform periodic penetration testing performed by third-party security experts to uncover hidden vulnerabilities. The customer will also use a third-party security platform to uncover any emerging threats and the vendor must provide suitable assistance in the patching process to ensure that any threats are mitigated within the times set out in the relevant industry standard.

An annual software development lifecycle should be provided to the customer. Any affected upgrades or feature enhancements should include a security report that demonstrates how code has been reviewed for potential security issues.

The vendor must be able to provide the customer with an incident response plan, this plan should be able to clearly communicate to the customer and acceptable procedure that the vendor will follow when responding to security incidents that involves their platform.

Vendors must agree to use strong encryption standards for data. For data in transit TLS, SSH or IPsec protocols should be used and for data at rest AES, RSA or Twofish encryption should be used with a minimum bit block size of 128 bits. Vendors should also be able to demonstrate the use of robust key management processes. The use of FTP technology is limited to Sftp only.

The customer requests that the vendor supply their access control policy for review, the intention is that the customer agrees that their processes for managing and monitoring access to their systems and data complies with agreed security standards. The policy should also demonstrate adequate steps to thwart risks posed by insider threats.

The vendor must be able to prove that they provide security awareness training for their employees and that they are conducted no less than twice a year.

Vendors that hold or transfer sensitive or personally identifiable data should ensure their compliance with data privacy regulations relevant to our industry or location, such as GDPR or HIPAA.

Adra requires that the vendor undergo regular audits by third-party organizations to ensure compliance with security standards and uncover any potential issues. These audit reports should be available for the customer to see on request.

Include specific security and performance standards within SLAs, and ensure they have penalties for non-compliance.

Understand their policy for software end-of-life and how they handle the transition without compromising security.

Vendors should provide assurance that their own supply chain is secure, particularly if they integrate third-party components into their software.

Request a comprehensive software inventory that includes all applications and their dependencies used in their infrastructure.

SaaS (vendor) Hosted Platform

User Interface

- Access to the UI must be done through a modern web browser, our preference would be Microsoft edge in native mode not IE compatibility mode.
- Access to the UI must be done via the browser over HTTPS and not utilise any non-standard ports.
- Our preference would be that any UI uses native technologies in the browser and not employ any extensions or plug ins except where it enhances the security of the access.

Security

Software as a Service (SaaS) vendors must adhere to these stringent set of practices to ensure their hosted platforms comply with security standards.

SaaS vendors should obtain and maintain certifications such as ISO/IEC 27001, SOC 1, SOC 2, and comply with industry-specific regulations such as PCI DSS for payment processing.

Vendors must agree to use strong encryption standards for data. For data in transit TLS, SSH or IPsec protocols should be used and for data at rest AES, RSA or Twofish encryption should be used with a minimum bit block size of 128 bits. Vendors should also be able to demonstrate the use of robust key management processes. The use of FTP technology is limited to Sftp only.

Vendors should conduct quarterly vulnerability assessments and scans to identify potential security weaknesses in their software and infrastructure. If the vendors software required an update, scans should be done after installation and prior to releasing the update to the production environment. This information should be shared with the customer either electronically or during account meetings.

The vendor must be capable of demonstrating a clear process for timely patch management, including the monitoring of vulnerabilities, assessment of risks, and the prompt deployment of patches, follow secure coding practices as part of the software development lifecycle (SDLC), including regular code reviews, static and dynamic code analysis, and integrating security into the code implementation pipeline. Adra would expect the vendor to prioritise patches based on the CVSS score and patch or mitigate critical vulnerabilities as soon as they become aware. The vendor will be expected to have a patch criticality matrix or equivalent available for the customer to review.

The vendor must employ strict access control measures, user authentication must use multi-factor authentication (MFA) with comprehensive role and attribute-based access controls. The vendor must provide the ability to perform regular access reviews and audits to ensure correct access is given to all users of the system leveraging least privilege access as a default role. Where applicable a method of providing single sign on with modern IDP providers such as Microsoft and Okta will be required. Any access to the system must provide a session timeout for logged in users to prevent stale account access.

Any vendor providing services to Adra must respect data privacy laws by ensuring data is stored and processed in accordance with the DPA2018 and the EU GDPR regulations.

Vendors have an incident response plan that includes notification processes for affected customers in case of a security breach. As a minimum these must prove that the vendor can keep the customers data secure and respond quickly and effectively to a breach and maintain a level of communication with the customer.

The vendor must be able to prove that they provide security awareness training for their employees on security best practices, including how to recognize and respond to security threats and that they are conducted no less than twice a year.

The customer expects a comprehensive and robust backup and disaster recovery strategy from the vendor. This strategy is vital to ensure data integrity and service continuity in the event of an incident. The strategy should demonstrate the backup process and frequency along with redundancy processes, be encrypted and utilise secure storage. Be highly available and provide the customer with selective restoration options. The vendor must ensure that there is a business continuity plan that addresses how services will be maintained in the event of a disaster or major incident, the plan must also address how communication is handled between the vendor and the customer during such an event.

Adra requires that the vendor undergo regular audits by third-party organizations to ensure compliance with security standards and uncover any potential issues. These audit reports should be available for the customer to see on request.

Secure application programming interfaces (APIs) against common threats as defined by the OWASP Top 10, such as injection attacks, broken authentication, and sensitive data exposure. Adra requires that vendors use and monitor a security information and event management system or as an alternative employ a third-party organisation to provide managed detection and response services over the hosted environment.

Provide customers with tools and policies that allow them to manage their data and understand how their data is being protected.

SLAs should include as a minimum an outline of the performance and availability metrics, including how security reports from a log monitoring system such as MDR or SIEM are produced and made available to the customer.

Clearly communicate end-of-life policies for services and how transitions are managed without compromising security.