Vendor Questionnaires

Unicis vendor questionnaire is based on MVSP controls and provides a clear set of requirements for enterprise-ready products and services.

Please answer each question with a *"yes"* or *"no"*, and provide a brief description of the process or controls in place if the answer is *"yes"*.

Please submit all the answers to as a `txt` or `md` file format or use the function to export to PDF.

1.1 External Vulnerability Reports

Do you have a process in place to accept and process external reports of security issues in your products and/or services?

If yes, please describe the process.

1.2 Customer Testing

Do you allow customers to safely and effectively perform testing against your products and/or services?

If yes, please describe the process.

1.3 Self-Assessment

Do you perform annual reviews of your application security controls for each qualifying product or service to identify corrective actions or areas of continued improvement?

If yes, please describe the process.

1.4 External Testing

Do you schedule and perform regular third-party penetration testing against your products and/or services?

If yes, please describe the process.

1.5 Training

Do you provide regular and ongoing security awareness training for your employees?

If yes, please describe the process.

1.6 Compliance

Do you identify and complete relevant compliance obligations based on your industry and regulatory requirements?

If yes, please describe the process.

1.7 Incident Handling

Do you have processes in place to ensure the smooth handling of security and privacy incidents?

If yes, please describe the process.

1.8 Data Handling

Do you have a process in place to handle data stored on removable or decommissioned hardware?

If yes, please describe the process.

2. Application Design Controls

2.1 Single Sign-On

Do you provide customers with the option to use single sign-on to access your product and/or service?

If yes, please describe the process.

2.2 HTTPS-only

Do you ensure sensitive data is encrypted in transit between the end-user and your product and/or service?

If yes, please describe the process.

2.3 Security Headers

Do you enforce appropriate browser protections within your product and/or service to protect against common web threats?

If yes, please describe the process.

2.4 Password Policy

Do you have a strong password policy in place to protect users who opt to use password-based authentication?

If yes, please describe the process.

2.5 Security Libraries

Do you use standardized libraries to improve the security of your product and/or service?

If yes, please describe the process.

2.6 Dependency Patching

Do you have processes in place to identify and maintain up-to-date components within your product and/or service?

If yes, please describe the process.

2.7 Logging

Do you store appropriate logs to assist with debugging and incident response activities?

If yes, please describe the process.

2.8 Encryption

Do you store sensitive data in an encrypted format?

If yes, please describe the process.

3. Application Implementation Controls

3.1 List of Data

Do you have information on the type and amount of data handled by your product and/or service available for threat modeling or incident response purposes?

If yes, please describe the process.

3.2 Data Flow Diagram

Do you have information on the flow of data through systems available for threat modeling or incident response purposes?

If yes, please describe the process.

3.3 Vulnerability Prevention

Do you provide training on common security issues to your development and quality assurance teams?

If yes, please describe the process.

3.4 Time to Fix Vulnerabilities

Do you patch identified vulnerabilities within a reasonable time frame, and inform customers where appropriate?

If yes, please describe the process.

3.5 Build Process

Is your build process fully scripted/automated and generating provenance?

If yes, please describe the process.

4. Operational Controls

4.1 Physical Access

Do you have physical security controls in place to protect sensitive data stored or accessible from trusted locations?

If yes, please describe the process.

4.2 Logical Access

Do you have logical access controls in place to protect sensitive data and limit access to authorized users?

If yes, please describe the process.

4.3 Sub-Processors

Do you understand where you may be sharing data with third-party sub-processors, and validate their security posture?

If yes, please describe the process.

4.4 Backup and Disaster Recovery

Do you have processes in place to ensure backup and recovery of your product and/or service in the event of a disaster?

If yes, please describe the process.