imperva

# SECURITY APPENDIX

This Security Appendix is part of and incorporated into the End User License Agreement available at https://www.imperva.com/legal/license-agreement/ at the time of purchase ("**Product and Services Agreement**"). Together, this Security Appendix and the Product and Services Agreement shall be the "**Agreement**". Capitalised terms used but not defined in this Security Appendix, shall have the meanings set out in the End User License Agreement.

## 1. DEFINITIONS

**End User Information** means data processed by the Imperva Products and Services pursuant to an Order.

**Security Incident** means a confirmed or reasonably suspected, accidental or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to End User Information.

## 2. GENERAL

2.1 Imperva maintains an information security management system (including a formally documented information security policy, IT security functions with clearly defined roles and responsibilities and processes) that complies with ISO/IEC 27001:2013, PCI DSS, SOC 2 Type II or such other alternative standard as it may elect from time to time.

2.2 An information security risk assessment is performed at least annually by Imperva on its critical information assets, information systems and processes relevant to the Imperva Products and Services to:

(i) identify the information security risks associated with the above mentioned critical information assets, information systems and processes; and

(ii) plan risk remediation activities for each identified information security risk, which include identification and implementation of appropriate mitigating controls and remediation timelines.

## 3. SECURITY INCIDENTS

3.1 If Imperva becomes aware of a Security Incident, Imperva will, without undue delay and as applicable: (1) notify End User of the Security Incident without undue delay and, in any event, within 48 hours; (2) investigate the Security Incident and provide End User with information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

3.2 Notification of a Security Incident will be provided to one or more of End User's points of contact by any means Imperva selects, including via email. It is End User's responsibility to ensure End User's points of contact maintain up to date and accurate contact information. End User is

responsible for complying with its obligations under applicable law, including any third party notification obligations related to any Security Incident.

3.3 Imperva's notification of or response to a Security Incident is not an acknowledgement by Imperva of any fault or liability with respect to the Security Incident.

3.4 Imperva maintains a record of security incidents with a description of the incident, the time period, the impacts of the incident, the name of the reporter, to whom the incident was reported, and the procedure for recovering data.

**4. AUDITS**

4.1 Imperva will conduct audits of the security of the computers and computing environment that it uses to process End User Information. Where Imperva is auditing to a standard or framework which provides for audits, an audit will be performed at least annually. Each audit will be performed according to the requirements of the regulatory or accreditation body governing the control standard or framework. Each audit will be performed by qualified, independent, third party auditors selected by Imperva at Imperva's expense.

4.2 Where appropriate, each audit will result in an audit report ("**Imperva Audit Report**"), which Imperva will make available to End User upon request, subject to End User signing an appropriate non-disclosure agreement to the extent Imperva considers this necessary. The audit report will be Imperva's Confidential Information. Imperva will promptly remediate issues raised in any audit report to the satisfaction of the auditor. The audit report will be subject to non-disclosure and distribution limitations of Imperva and the auditor.

4.3 To the extent End User's audit requirements cannot reasonably be satisfied through an Imperva Audit Report, documentation or other information Imperva makes generally available to its End Users, Imperva will promptly respond to End User's additional audit instructions. Before the commencement of an additional audit initiated by End User, the Parties will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Imperva to unreasonably delay performance of the audit. Such an audit will be conducted by an independent, accredited third party audit firm, during regular business hours, with reasonable advance notice to Imperva, and subject to reasonable confidentiality procedures. Neither End User nor the auditor shall have access to any data from Imperva's other end users or to Imperva systems or facilities not involved in the Imperva Products and Services. End User understands that some of Imperva's subprocessors may not permit inspection of their facilities. End User is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any time Imperva expends for such audit, in addition to the rates for services performed by Imperva.

4.4 Imperva logs, or enables End User to log, access and use of information systems containing End User Information, registering the access ID, time, authorization granted or denied, and relevant activity.

5. **BUSINESS CONTINUITY**

5.1 Imperva will implement and maintain at all times adequate business continuity planning in respect of its own business activities to the extent relevant to the provision of Imperva Products and Services to End Users. Such arrangements shall:

5.1.1 contain a description of recovery strategies and processes for the infrastructure supporting the Imperva Products and Services;

5.1.2 be developed and reviewed in accordance with recognised industry standards; and

5.1.3 be reviewed and updated at least annually.

5.2 Imperva's redundant storage and its procedures for recovering data are designed to attempt to reconstruct End User Information in its original or last-replicated state from before the time it was lost or destroyed.

**6. PERSONNEL**

6.1 Imperva personnel are subject to background screening, subject at all times to applicable law.

6.2 Imperva personnel receive both an initial and ongoing training awareness program that addresses relevant security procedures and their respective roles.

**7. ACCESS CONTROL**

7.1 Imperva maintains and updates a record of personnel authorized to access Imperva systems that contain End User Information.

7.2 Imperva deactivates authentication credentials that have not been used.

7.3 Imperva specifies personnel who may grant, alter or cancel authorized access to data and resources.

7.4 Imperva ensures that where more than one individual has access to systems containing End User Information, the individuals have separate login credentials.

7.5 Imperva restricts access to End User Information to only those individuals who require such access to perform their job function.

7.6 Imperva instructs Imperva personnel to disable administrative sessions when leaving premises Imperva controls or when computers are otherwise left unattended.

7.7 Imperva stores passwords in a way that makes them unintelligible while they are in force.

7.8 Imperva uses recognised industry practices to identify and authenticate users who attempt to access information systems.

7.9 Where authentication mechanisms are based on passwords, Imperva requires that the passwords are renewed regularly.

7.10 Imperva ensures that de-activated or expired identifiers are not granted to other individuals.

7.11 Imperva monitors, or enables End User to monitor, repeated attempts to gain access to the information system using an invalid password.

7.12 Imperva maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

7.13 Imperva uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed.

7.14 Imperva has controls to avoid individuals assuming access rights they have not been assigned to gain access to End User Information they are not authorized to access.

**8. PHYSICAL SECURITY**

8.1 Imperva ensures the information systems used to provide Imperva Products and Services and which handle End User Information are located in secured locations.

8.2 Imperva limits access to facilities where information systems used to provide Imperva Products and Services and which handle End User Information are located to identified authorized individuals.

**9. MALWARE AND VULNERABILITY MANAGEMENT**

9.1 Systems are hardened and deployed with robust baseline security standards based on industry best practices.

9.2 Security configuration is reviewed against internal standards on an annual basis at a minimum to monitor compliance.

9.3 Imperva routinely scans its network and applications for potential vulnerabilities and takes action based on recognized industry guidelines to address any discovered issues

9.4 Security patches are assessed and prioritized according to their severity and business impact, tested before deployment and deployed according to severity in a timely manner to counter latest security vulnerabilities exploitation.

9.5 Penetration tests are conducted at least annually on all external or internet facing systems.

**10. SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

10.1 Change requests must be initiated through a formal change request process, which includes risk and impact analysis in proportion to the proposed change.

10.2 Change requests are approved by an appropriate level of management. For emergency changes, prior notification or escalation to change management stakeholders is maintained.

10.3 Security requirements are given due consideration in the systems development and change management processes.

10.4 System development follows industry secure coding best practice.

10.5 User Acceptance Testing (UAT) and System Integration Testing (SIT) test plans are prepared and their results are approved by an appropriate level of management upon completion of testing.

10.6 Imperva maintains separate system environments for production and non-production environments.

10.7 Imperva maintains an adequate segregation of duties, as defined by role, to allow the minimum possible access by its technical teams, whether employee, contractor or management.

**11. NETWORK SECURITY**

11.1 Imperva encrypts, or enables End User to encrypt, End User Information that is transmitted over public networks.

11.2 Wireless networks are configured with appropriate authentication mechanisms.

11.3 Imperva operates recognised industry practice with respect to cryptographic key management. Further information on the controls implemented is available upon request.

**12. CERTIFICATIONS**

12.1 Details of the certifications available for Imperva Products and Services are available here from time to time.

**13. SOFTWARE**

13.1 If an issue cannot be analysed and/or corrected via telephone or via e-mail, Imperva will require End User to permit use of a screen sharing application to allow for Support to be performed. End User may stipulate such commercially reasonable controls as it requires in respect of the utilisation of such a screen sharing app.

**14. OTHER**

14.1 End User is responsible for ensuring that it complies with applicable law. End User acknowledges that Imperva is neither responsible for determining which laws or regulations are applicable to End User nor whether Imperva's provision of the Imperva Products and Services meets or will meet the requirements of such laws or regulations.

14.2 In the event of any conflict or inconsistency between this Security Appendix and the Products and Services Agreement, the Products and Services Agreement shall prevail.