Adevinta Vendor Minimum Security Requirements (Public Document)

Addendum

REVISED VERSION

Purpose

The Vendor Minimum Security Requirements (“MSRs”) set out in this Addendum (“Addendum”) cover key security-related areas designed to protect the confidentiality, integrity, and security of (i) information which is held, stored, transmitted or processed by or on behalf of Adevinta, and (ii) Adevinta’s IT networks and systems..

References in this Addendum to “Vendor” shall apply to and be binding on the person supplying goods and/or services to Adevinta under the agreement which expressly references this Addendum (“Agreement”). For the purposes of this Addendum, “Adevinta” shall mean the entity which is an affiliate or subsidiary of Adevinta ASA which is entering into the Agreement and includes all its affiliates and subsidiaries of Adevinta (as applicable). This Addendum shall be deemed to be included in and form an integral part of the Agreement, provided that where the Agreement or an agreement related to the Agreement (including any Data Privacy Agreement) expressly provides for specific standards, measures, processes, rights, obligations or remedies relating to the subject matter of this Addendum, those specific items shall govern.

Policy Requirements:

These MSRs are further supported by the Adevinta Global Information Security security policies. Adevinta believes that policies and procedures play an important role in the effective implementation of enterprise-wide information security and the success of the resulting security measures employed to protect information and information systems.

The Vendor must develop and promulgate formal, documented policies and procedures governing these MSRs and must ensure their effective implementation.

Adevinta Service Level Agreement ("SLA") Mandatory Remediation Requirements for MSRs and Security Policies:

The following table describes the priority rating, threat level characteristics and remediation window required by the Vendor to address identified vulnerabilities in developed and supported Adevinta applications:

Vulnerability Priority	CVSS	Characteristics	Remediation Window
P1	8.0 - 10.0	Any issue in internally developed software with no compensating controls that could result in material loss, regulatory failure, excessive damage to brand or excessive damage to users (examples include, but not limited to: XSS, XSRF, SQL injection). A vulnerability being actively exploited or high exposure to a significant or immediate exploit of any company managed public facing site and/or company data. High risk vulnerability that is publicly known or likely to become public with a high public relations impact.	Max 5 calendar days
P2	7.0 - 7.99	Issues that do not pose an immediate direct risk that could result in material loss, regulatory failure, excessive damage to brand or excessive damage to users. Issues where compensating controls are deemed satisfactory for the duration of the SLA. Exploitation of this risk would still result in significant loss.	Max 30 calendar days

P3	5.0 - 6.99	Issues that have low impact to Adevinta's customers or customer service and do not have direct brand, financial, customer experience or service delivery impact. An issue that is contrary to security engineering best practices.	Max 45 calendar days
P4	1.0 - 4.99	Vulnerabilities deemed to be unlikely to be exploited without extensive insider knowledge. Exploitation would not result in significant damage.	Max 90 calendar days

Minimum Security Requirements

Access Control (AC):

Vendors must limit information system access to authorized users, processes acting on behalf of authorized users, or devices and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT):

Vendors must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that designated personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability (AU):

Vendors must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. As determined Adevinta may request evidence of audit and accountability processes via documentation or via planned site visits.

Security Assessments (CA):

Vendors must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM):

Vendors must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP):

Vendors must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication (IA):

Vendors must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response (IR):

Vendors must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Vendors must comply with all applicable European Union (EU) requirements, such as the EU GDPR (General Data Protection Regulation) requirements.

Vendors must notify the Adevinta CSIRT (csirt@adevinta.com) in a timely manner of any significant incidents or reports to a regulatory authority (that may impact on the services provided to Adevinta or that may impact Adevinta).

Maintenance (MA):

Vendors must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP):

Vendors must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection (PE):

Vendors must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Security Planning (PL):

Vendors must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security (PS):

Vendors must: (i) ensure that individuals occupying positions of responsibility within Vendors (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment (RA):

Vendors must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition (SA):

Vendors must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection (SC):

Vendors must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, that promote effective information security within organizational information systems.

System and Information Integrity (SI):

Vendors must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.