Alludo Vendor Security Requirements

Contents

Introduction

This document outlines the information security, business continuity, and privacy practices of the companies in the Alludo group (collectively "Alludo"), as well as the program for evaluating the security and continuity measures of the vendors of Alludo. The processes, procedures, requirements and obligations referred to herein are collectively the "Alludo Standards".

This **Vendor Security Requirements Document** informs those vendors providing goods and services ("Vendors") of the security, business continuity, and privacy expectations that Alludo holds them accountable for when providing services. Vendors must implement these requirements following industry best practices and their corporate security policies, Alludo will not be liable for any issues vendors face, including data loss or equipment damage, regardless of cause.

In case of any inconsistencies between this document and a written agreement, the terms of the written agreement will take precedence. Vendors must also comply with any local, national, or regional regulatory requirements. If a conflict arises between this document and applicable regulations, vendors should notify Alludo and suggest alternate controls to maintain equivalent security, continuity, or privacy standards.

Overview of Vendor Security Requirements

Alludo has a responsibility to protect its restricted and confidential information from unauthorized access or disclosure. For this, Alludo implements the Alludo Standards - internal information security, business continuity and privacy standards to ensure that such restricted and confidential information is protected and that the services provided by Alludo are continuously available. To ensure Alludo's compliance with internal standards and regulatory requirements relating to information security and business continuity, Alludo requires that its Vendors adhere to the Alludo Standards outlined in this document.

In turn, to the extent a Vendor delegates or subcontracts any portion of Vendor's obligations under its agreement with Alludo, or, engages another vendor to provide services directly or indirectly to Alludo, the Vendor shall require such vendor to implement and administer an information protection program and plan that complies with Alludo Standards. Alludo is committed to reasonably working with its Vendors to help the Vendor meet compliance requirements relating to Alludo Standards. The extent of the applicability of such Alludo Standards to a particular Vendor will vary depending on the type of service and products provided by such Vendor to Alludo.

Identity and Access Control

Vendor shall ensure:

1. **Access Control and User Management**:
   1.1. A documented access control policy is in place and reviewed at least annually.
   1.2. User roles, permissions, and access rights are defined and documented.
   1.3. Standard processes for user onboarding and offboarding are in place, including record-keeping of relevant approvals.
   1.4. Access to IT infrastructure components is granted based on the least privilege principle and managed through identity management tools (e.g., Active Directory, OKTA or similar).
   1.5. Individual access to systems, network resources, and other IT resources is formally approved and controlled through unique User IDs and individual passwords.
   1.6. Segregation of duties is maintained while creating/amending user IDs and allocating privileges.

2. **Password and Authentication Policies**:
   2.1. Users are required to change their password upon initial sign-on.
   2.2. Passwords meet industry-standard requirements, including length, expiry, complexity, password history, failed attempts, account lockout duration, password age, and change on first logon.
   2.3. Secure mechanisms are used to deliver user passwords and validate user identities before initiating password resets.
   2.4. Systems that do not support IdP authentication or are required to be built standalone are configured to enforce strong authentication, no less than the configuration defined in central password and access control policies.
   2.5. All systems and applications are configured to use secure log-on procedures via approved identity and access management mechanisms.
   2.6. Systems and applications are configured for idle session timeout to prevent unauthorized access.

3. **Privileged Access Management**:
   3.1. Privileged access to resources is restricted to defined user roles and approved by authorized personnel.
   3.2. Privileged user accounts are configured to use multifactor authentication.
   3.3. Privileges that are no longer required are revoked immediately.
   3.4. Use of administrative credentials is restricted to limited circumstances such as troubleshooting, and users perform day-to-day operations with least privileged credentials.
   3.5. Access to critical IT infrastructure, systems, network devices, and applications (e.g., remote access, critical servers, network devices) is protected using multifactor authentication.

4. **Access Review and Monitoring**:
   4.1. Periodic access rights reviews are carried out, and identified exceptions are addressed promptly.
   4.2. A reconciliation of all user IDs (including domain, applications, network devices, IT systems, middleware, databases, etc.) is conducted no more than annually, with immediate corrective actions taken for any identified discrepancies.

5. **Third-Party and Vendor Management**:
   5.1. Third-party vendor access to networks and systems is strictly controlled, based on need-to-know and formal approval.
   5.2. Vendor-supplied default credentials are changed before systems, applications, network devices, or other IT infrastructure devices are put into production.

6. **Special Access Considerations**:
   6.1. Generic and shared IDs are not used unless formally justified and approved by senior management, with mechanisms to track usage and trace actions to individuals.
   6.2. All non-console administrative access is encrypted using industry-approved encryption algorithms, and insecure protocols (e.g., telnet/ftp) are prohibited for non-console administrative access.

Asset Management

Vendor shall ensure:

7. **Asset Management and Inventory**:
   7.1. Comprehensive asset inventories are maintained, capturing essential details such as asset owner information, contact data, and location.
   7.2. Records of Information Technology assets, including hardware, operating systems, applications, and databases, are regularly updated and reviewed to ensure accuracy.
   7.3. Asset management procedures and configuration controls are established and maintained to manage the availability of critical assets and the configurations of vital network and information systems.

8. **Information Classification and Labeling**:
   8.1. An information classification policy with supporting procedures and guidelines is maintained. All assets are labeled according to established instructions, and information is classified and protected based on defined classification levels.

9. **Asset Handling**:
   9.1. Asset management guidelines for proper handling are maintained and communicated to all applicable employees and contractors.
   9.2. Documented procedures are in place for safeguarding information assets, identifying assets due for disposal, and ensuring secure disposal of such assets.
   9.3. Processes are established to ensure that allocated assets are promptly returned to the corresponding asset management team upon termination or separation of employment, contract, or agreement.

10. **Mobile Device and Removable Media Management**:
    10.1. Policies and procedures for controlling mobile devices (including BYOD) used to store, transmit, or process business information are implemented. Adequate protection measures are required before allowing mobile devices access to business information and resources.
    10.2. The use of removable mass storage devices must be encrypted to ensure data security.

11. **Software Compliance**:
    11.1. The use of unlicensed or unapproved software is prohibited. Processes are in place to identify any violations and take necessary actions to address them.

IT Operations

Vendor shall ensure:

12. **Critical System Operations**:
    12.1. Procedures for operating critical networks and information systems are established and maintained, encompassing:
        12.1.1. Formal approval processes for IT asset access.
        12.1.2. Robust authentication mechanisms for all technologies (e.g., VPN, Windows logon).
        12.1.3. Regular review of privilege entitlements.
        12.1.4. Identification of network locations for critical technologies based on business continuity requirements.
13. **Change Management**:
    13.1. A comprehensive change management process is implemented for IT systems, applications, databases, and network components, ensuring:
        13.1.1. Logging, review, testing, and formal approval of all changes.
        13.1.2. Rollback plans for potentially disruptive modifications.
14. **Other**:
    14.1. Systems and network components handling sensitive and confidential information are subject to file integrity monitoring checks.
    14.2. All systems and network components are configured to use authorized Network Time Protocol (NTP) sources for accurate time synchronization.
    14.3. Regular proactive and preventive maintenance processes are established for all critical systems, applications, network devices, and end-user machines.
    14.4. Firewall and router rule sets are reviewed periodically or as per industry standards, with unnecessary or unauthorized rules promptly removed.
    14.5. Controls are implemented to maintain the integrity of information and software throughout the IT environment.

Human Resource Security

Vendor shall ensure:

15. **Background Checks**:
    15.1. Establish and maintain policies and procedures for conducting background checks.
    15.2. Perform appropriate background checks on employees and contractors before onboarding, to the extent legally permitted, based on their duties and responsibilities.
16. **Personnel Change Management**:
    16.1. Implement a process to manage changes in personnel or their roles and responsibilities, including educating new personnel on relevant policies and procedures.

16.2. Revoke access rights, badges, equipment, and other resources promptly following personnel changes when they are no longer necessary or permitted.

17. **Policy Enforcement**:
    17.1. Implement and uphold a clear disciplinary process for employees who breach security policies.
    17.2. Ensure accountability for security policy violations through appropriate contractual measures. This includes incorporating relevant clauses in employment contracts for staff and service agreements for third-party contractors.

Security and Privacy Training

Vendor shall ensure:

18. Security and privacy training is mandatory for all employees and contractors. This training must be completed upon initial hire and annually or less thereafter.
19. Employees and contractors with significant IT security responsibilities undergo specialized annual training tailored to their specific security roles and duties.
20. Management has access to tools and systems that allow them to monitor and track the training progress of their employees and contractors.
21. The organization's training and awareness program undergoes periodic review and updates. This process considers evolving business requirements, changes in legislation, and lessons learned from past security incidents.

Information Security & Governance

Vendor shall ensure:

22. **Security Framework and Governance**:
    22.1. The vendor must implement a recognized security standard framework (e.g., NIST CSF, RMF, 800-53, ISO 27001, CIS) for information and cybersecurity governance. This framework should include:
        22.1.1. Comprehensive information and cybersecurity policies and procedures, subject to annual review, formal approval, and organization-wide communication.
        22.1.2. A well-defined information security strategy aligned with business objectives.
        22.1.3. Robust governance and risk management processes specifically addressing information and cybersecurity risks.
        22.1.4. Compliance mechanisms to meet legal and regulatory requirements pertaining to information and cybersecurity.
    22.2. If not adhering to a recognized security framework, the vendor must submit a report demonstrating that their environment has undergone an audit.
        22.2.1. A remediation plan for identified issues, including expected timeframes, should be mutually agreed upon between the vendor and Alludo.

23. **Leadership and Organizational Structure:**
    23.1. Appropriate roles and responsibilities for Information and Cyber Security are defined and implemented throughout the organization.

24. Risk Management and Assessment:

24.1. A formal risk management framework approved by Senior Management is in place for:

24.1.1. Identifying both internal and external threats.

24.1.2. Assessing sensitivity of information/data in scope.

24.1.3. Evaluating potential business impacts.

24.1.4. Assessing threats, vulnerabilities, and corresponding risks.

24.1.4.1. All identified risks and threats are prioritized, with timely action taken to mitigate risks accordingly.

24.1.4.2. Processes and/or tools are implemented to identify events that cause interruptions to the organization's key business purposes.

24.1.4.3. The vendor must notify Alludo immediately if unable to remediate or reduce any material risk that could impact the provided service.

25. Compliance and Performance Monitoring:

25.1. Processes are in place to identify, record, and track all applicable legal, regulatory, and contractual requirements for the organization.

25.2. Periodic assessments are performed to validate compliance with legal, regulatory, and contractual obligations. Records are maintained for such assessments and identified gaps are mitigated without undue delay.

25.3. Policies, procedures, and guidelines are reviewed at least annually and updated as per the legal, regulatory, and contractual requirements.

25.4. Key Performance Indicators for critical functions such as IT, Information Security and Data Privacy etc. are defined, formally documented, periodically assessed, and reported to Sr. management.

Network Security

Vendor shall ensure:

26. Network Design and Security Architecture:

26.1. The vendor network employs "defense in depth" principles, incorporating appropriate controls like network segmentation to minimize information and cybersecurity breaches.

26.2. Strong architectural design is implemented, featuring effective identity management and robust operating system configurations.

26.3. The network design and implementation undergo annual reviews to ensure ongoing effectiveness and security.

26.4. The network configuration complies with all applicable legal and regulatory requirements.

27. Access Control and Authentication:

27.1. External network connections must be documented, routed through firewalls, verified, and receive approval prior to being established.

27.2. Wireless network access requires authentication, authorization, segmentation, and encryption. Systems are in place to detect and respond to rogue wireless access points or unauthorized connections.

27.3. Remote access to the vendor network must be approved and conducted via secure means, with multifactor authentication.

27.4. Controls are implemented to prevent or minimize unauthorized access to the vendor network.

28. **Secure Administration and Management:**
    28.1. All management-related network traffic between administrative workstations and network devices uses industry-standard encryption and authentication protocols.
    28.2. Non-console administrator access occurs exclusively through industry-approved encrypted channels.
    28.3. Guest accounts are disabled or removed, and all default, and vendor-supplied passwords are changed before network devices are deployed in the production environment.

29. **Network Hardening and Threat Protection:**
    29.1. Unused services, applications, and ports are disabled to reduce the attack surface.
    29.2. Intrusion detection and/or prevention measures are deployed for critical network segments.
    29.3. Critical systems are safeguarded against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

Cryptography

Vendor shall ensure:

30. A comprehensive cryptographic policy, along with supporting procedures, is implemented to ensure compliance with all relevant legal, regulatory, and business requirements. This policy follows industry best practices to guarantee secure encryption in accordance with applicable laws and standards.

31. **Encryption Standards and Implementation**:
    31.1. Only secure, industry-approved encryption algorithms and key strengths are permitted, guaranteeing adequate data protection across all systems and processes.
    31.2. Cryptographic solutions are implemented to protect confidential information and restrict access to sensitive data, including encryption for data both in transit and at rest.
    31.3. All password storage and transmission is encrypted, maintaining the confidentiality of user credentials at all times.
    31.4. Alludo data in transit must be encrypted (TLS 1.2 at a minimum or newer standard).
    31.5. Alludo data at rest must be encrypted (AES 256-bit at a minimum or newer standard).

Data Security

Vendor shall ensure:

32. **Recovery:**
    32.1. **Data Backup and Recovery**:
        32.1.1. Backups of Alludo data must be performed periodically.
        32.1.2. Backups of Alludo data must be retained for 1 year.

32.1.3. Backups of Alludo data must be encrypted.

32.2. **Disaster Recovery**:

32.2.1. Disaster recovery plan must be tested annually.

33. **Backup Policy and Procedures**:

33.1. Backup policy and supporting procedures must be clearly documented.

33.2. Backup restoration processes must be documented and tested at defined frequency.

33.3. Evidence of backup restoration testing must be maintained.

33.4. A copy of critical data backup files must be kept secured.

34. **Backup Monitoring**:

34.1. Logs for failed backups (if any) must be monitored by backup admin.

34.2. Corrective actions for failed backups must be performed and documented.

35. **Data Location**:

35.1. Vendor is responsible for ensuring compliance with all applicable data protection and privacy laws in the countries where the data will be stored.

35.2. Adhere to restrictions on transferring data across borders (GDPR, etc.).

35.3. Vendor must implement appropriate technical and organizational security measures to protect the data, in accordance with the laws and standards of the countries where the data is stored.

35.4. Alludo reserves the right to audit the vendor's data handling practices to ensure compliance with agreed-upon security measures and local regulations.

36. **Deletion of Data**:

36.1. Procedures for secure data deletion upon contract termination must be in place, ensuring compliance with local data retention laws.

37. **Full Disk Encryption**:

37.1. Full disk encryption must be configured for workstations and servers.

38. **Data Classification**:

38.1. A documented data classification policy must be in place.

38.2. Data must be classified based on its criticality and sensitivity.

38.3. Security controls corresponding to the sensitivity of data must be identified and implemented.

Information Communication

Vendor shall ensure:

39. **Web Security**:

39.1. Web content filtering software is implemented to block access to websites hosting malicious content.

39.2. All web-based systems and applications must be accessed via secure and authenticated mechanisms.
39.3. Client-server communication for applications and web portals must occur over encrypted channels.

40. **Email Security**:
    40.1. Security controls are in place to prevent misuse of the email system.
    40.2. All email communications must be transmitted over encrypted channels.
    40.3. Email gateway is equipped with:
        40.3.1. Anti-phishing filters.
        40.3.2. Enable security protocols for email (i.e. DMARC, DKIM and SPF).
        40.3.3. Other necessary configurations to prevent email-borne threats.

Software Development

Vendor shall ensure:

41. **Software Development Lifecycle**:
    41.1. An established Software and Systems development framework must be in place.
    41.2. Systems and applications must be developed following Secure Software Development best practices (e.g., OWASP).
    41.3. Software code must be:
        41.3.1. Protected from unauthorized modification
        41.3.2. Securely stored
        41.3.3. Subject to Quality Assurance processes
    41.4. Code reviews must be performed.

42. **Testing and Deployment**:
    42.1. Applications must undergo thorough security and functionality testing before deployment to the production environment.
    42.2. Production and non-production environments must be appropriately segregated.
    42.3. Segregation of duties between production and non-production development must be maintained.
    42.4. Production data should not exist in a test environment.

Application security

Vendor shall ensure:

43. **Application Security:**
    43.1. Application security assessments are conducted for all newly developed applications and any existing applications undergoing significant changes to identify known security vulnerabilities.
    43.2. All identified security vulnerabilities with a CVSS score greater than 4 are mitigated before deploying the application to the production environment.

43.3. Code review processes are implemented to identify and remediate code that may introduce security vulnerabilities.

44. **Web Application Protection:**
    44.1. Public-facing web applications are safeguarded by a robust web application firewall to prevent external threats.

Patch Management

Vendor shall ensure:

45. The latest security patches are applied to systems, networks, applications, and databases etc. in a timely manner and based on criticality of the vulnerability addressed by the patch. Patches are obtained from respective OEMs directly for proprietary systems.
46. All patches are tested before deployment of the patches to production systems and the correct operation of the patched service are verified after any patching activity.
47. Appropriate mitigations are in place if a system cannot be patched, effectiveness of such mitigations is assessed periodically, and corresponding evidence maintained.

Malware Protection

Vendor shall ensure:

48. All IT systems are continuously safeguarded by a malware protection solution that inspects incoming data in real-time to prevent service disruptions or security breaches. Additionally, proper user awareness procedures are enforced. The anti-malware system detects various threats including, but not limited to, viruses, spyware, worms, unauthorized mobile code, keyloggers, botnets, and trojans.
49. Malware signatures are regularly updated to ensure that systems are always equipped with the latest threat definitions.
50. The malware protection software is configured to perform both scheduled and on-demand scans, and to isolate or delete any identified malicious files or software.
51. End users do not have the rights or ability to disable the malware protection.

Vulnerability Management

Vendor shall ensure:

52. **Vulnerability Management Process**:
    52.1. Established policies, processes, and procedures for comprehensive vulnerability management.
    52.2. Processes to receive, analyze, and respond to vulnerabilities from both internal and external sources.

53. **Vulnerability Assessment and Remediation:**
    53.1. Quarterly vulnerability assessments on vendor's IT infrastructure and applications, including disaster recovery sites.
    53.2. Remediation of identified vulnerabilities with CVSS score greater than 4 within defined timelines.

54. Penetration Testing:

54.1. Annual independent penetration tests on vendor's IT infrastructure and applications used for Alludo services.

54.2. Tests aim to identify exploitable vulnerabilities and prevent security breaches through cyber-attacks.

54.3. Alludo granted access to relevant penetration/vulnerability test reports upon reasonable request.

Logging and monitoring

Vendor shall ensure:

55. Critical systems including applications are set to log key events (including those of privileged access and user activity) and retain such for a minimum period of 1 Year or as per applicable regulatory requirements.

56. As a minimum the logs from key events (as appropriate) contain the following:

56.1. System start-up and shutdown.

56.2. Start and stop status of critical services and processes.

56.3. Changes in the configuration parameter e.g., changes in system boot configuration.

56.4. Successful logins and Failed login attempts.

56.5. Creation, modification, and deletion of user accounts.

56.6. System/resources accessed.

56.7. Identification and location of who accessed the resources and from where.

56.8. Date and timestamp.

57. Audit logs are collected and correlated from multiple sources and sensors and stored securely and are tamper-proof to enable the reconstruction of such events.

58. Processes for monitoring log events (preferably real time) are established to detect any unauthorized activities, attack targets, and ensure that logs of key events are reviewed.

Incident management

Vendor shall ensure:

59. Roles and processes are clearly defined to ensure a prompt, effective, and organized response to information security and privacy incidents.

60. Employees and contractors are trained to recognize what constitutes a security incident, as well as how and where to report any potential or confirmed incidents.

61. Personnel responsible for analyzing and responding to incidents are qualified in the subject and undergo regular training on effective incident response practices.

62. A repository is maintained for all reported incidents, detailing actions taken to mitigate the incident’s impact and lessons learned from the event.

63. Alludo is notified as soon as the organization becomes aware of any security incident affecting them, but no later than 24 hours after detection.

Physical and Environmental Security

Vendor shall ensure:

64. Policies and procedures for physical security and environmental controls, aligned with industry standards, are implemented.
65. Critical facilities housing IT systems, applications, and personnel (e.g., data centers, operational sites) are protected from accidents, attacks, and unauthorized access.
66. Security measures like electronic access controls, identity verification, security guards, visitor management, and 24/7 CCTV monitoring are in place to prevent unauthorized entry.
67. CCTV footage is retained for at least 30 days, or longer if required by legal regulations.
68. Access to facilities is restricted to authorized personnel for specific purposes and regularly reviewed.
69. Visitors are escorted, their entry and exit times are logged, and they must wear visitor IDs at all times. Access cards or keys are collected upon departure.
70. Critical facilities are safeguarded against power loss using uninterruptible power supplies (UPS) or generators to ensure continuous operations.
71. Periodic maintenance is conducted on critical equipment like UPS, generators, smoke detectors, fire suppression systems, and access control systems, with records kept.
72. Facilities are built with fire-proof materials and equipped with fire alarms, smoke detectors, temperature and flood sensors, and fire extinguishers to protect against natural hazards.
73. Secure disposal mechanisms for data in both hard and soft copy formats are defined, using cross-cut shredders for paper and methods like sanitization, degaussing, or destruction for electronic media.
74. A clear desk policy ensures secure handling of Post-it notes, written documents, and removable media.
75. Physical and environmental controls are evaluated at least annually for effectiveness

Privacy and Data Protection

If the Vendor or its sub-processors processes personal data on behalf of Alludo or Alludo's customers, Vendor shall ensure the following:

76. **Data Privacy Compliance and Governance:**
    - 76.1. Comply with all applicable data protection laws.
    - 76.2. Establish a privacy management framework including:
        - 76.3. Privacy policies, statements, notices, and procedures (reviewed annually).
        - 76.4. Privacy governance and risk management processes.
        - 76.5. Adherence to legal and regulatory requirements.
    - 76.6. Maintain up-to-date records of processing activities for Alludo's personal data.
    - 76.7. Define and implement appropriate roles and responsibilities for Data Privacy:
        - 76.8. Appoint a senior Data Privacy Officer (or equivalent).
        - 76.9. Establish a specialist Data Privacy function.
        - 76.10. Form a committee to coordinate Data Privacy Compliance activities.

77. **Data Protection and Security Measures**
    - 77.1. Implement industry-standard safeguards (e.g., ISO/IEC 27001:2013, SOC2, etc) to

protect Alludo's information.

77.2. Apply additional safeguards for sensitive personal data (e.g., encryption, pseudonymization).

77.3. Enforce access controls:

77.4. Restrict access on a need-to-know and least privileged basis.

77.5. Promptly remove access rights upon termination or role changes.

77.6. Conduct periodic access rights reviews.

77.7. Ensure confidentiality commitments from all personnel processing Personal Data.

78. **Data Subject Rights Management:**

78.1. Assist Alludo in fulfilling Data Subject rights obligations.

78.2. Notify Alludo within 2 days of receiving Data Subject requests.

78.3. Respond to requests only as instructed by Alludo, unless legally required otherwise.

79. **Incident Response:**

79.1. Notify Alludo within 24 hours of personal data breaches involving Alludo data.

Sub-Contracting Measures

Vendor shall ensure:

80. They are conducting annual third-party risk assessments on all sub-processors involved in handling, processing, or storing Alludo data. These assessments should evaluate the sub-processors security controls, data protection measures, compliance with relevant regulations, and overall risk posture. Vendors must provide documentation of these assessments upon request, promptly address any identified risks, and communicate any changes to sub-processors or significant findings in a timely manner. We reserve the right to review assessment results and request additional security measures if necessary.

Business Continuity Management

Vendor shall ensure:

81. A Business Continuity Management (BCM) Policy is established, accompanied by detailed plans and procedures. These documents outline the organization's business continuity objectives and undergo annual review and approval.
82. A BCM testing framework is developed and implemented to evaluate the effectiveness of existing business continuity strategies.
83. Business Impact Analyses (BIA) are conducted at least annually or following significant organizational changes.
84. A crisis management plan is established, including specific provisions for pandemic preparedness. This plan ensures appropriate response to emergencies, focusing on protecting employees, visitors, the environment, assets, and maintaining critical business operations.
85. The Business Continuity Management System (BCMS) undergoes annual effectiveness testing, with detailed records maintained for each test.

<End of Document>