Ivanti Supplier Security Requirements

Contractors

Ivanti is committed to protecting our customers and employees through strong Information Security practices. As such, it is imperative that our suppliers and their constituents (collectively "Supplier") demonstrate the same commitments by meeting or exceeding Ivanti's security requirements to protect the data we entrust to them.

This document outlines Ivanti's Security Requirements for Suppliers that provide people resources (hereinafter "Contractors") to Ivanti that support business operations. This includes any Supplier that provides resources who perform Work at Ivanti facilities, on Ivanti system, or otherwise interact with Ivanti Data.

These requirements also apply to any sub-contractors, suppliers, or other constituents that support the Supplier when they are performing any activity or work for or on behalf of Ivanti (hereinafter "in-scope work").

In the event that the supplier is providing additional services, the Supplier may be required to agree to an additional Supplier Security Requirement document. In the case of conflict between Ivanti Supplier Security Requirements, the most stringent requirements apply.

Definitions

Ivanti Data – All data owned and/or licensed by Ivanti, data disclosed to Supplier by Ivanti, and work/work products produced under the applicable services agreement and/or statement of work.

In-scope Services – Any software or service that is being provided to Ivanti by the Supplier.

Information Resource – Any device that computes, transmits, processes, stores, or otherwise interacts with digital data.

Intellectual Property – This document limits "Intellectual Property" to mean source code for Ivanti's products, internal product notes, architecture diagrams, bug notes, or any other non-public information that could aid an external party replicate Ivanti's products.

Data Breach – A breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other processing of Ivanti Data transmitted, stored, or otherwise processed under the governing Master Services Agreement and/or Scope of Work.

Work – Any work or services provided provide by Supplier under the applicable services agreement and/or statement of work.

Vulnerability Scan – A process that identifies vulnerabilities in Information Resources or the software (including Operating System) on the Information Resource. Vulnerability that are identified by Vulnerability Scans are typically resolved by updating software or making configurations changes. Vulnerability scans are typically automated.

Penetration Test – A process that seeks to obtain access to sensitive Information Resources or Data by identifying weaknesses in security controls and network defenses. Penetration Tests are performed by

security personnel trained in bypassing security controls and may be assisted by tools and automation, but not completely automated.

Account – A digital identity that is used to perform work on an Information Resource. Accounts utilize a unique identity, such as a username or user number and are protected by an Authenticator to verify the user of the Account.

Service Accounts – A digital identity that is explicitly created to perform tasks within a system that does not require user interaction. Service Accounts typically have privileges on a system or service that are higher than a normal user.

Data Center – A centralized facility for Information Resources, especially those that are used to provide services to users as opposed to a day-to-day terminal or workstation.

Information Security Program – A set of practices that an organization implements to protect the Confidentiality, Integrity and Availability of information assets, including nondigital assets, typically documented in the form of Policies, Standards, and Procedures.

Information Security Program and Governance

1. Supplier must have a documented Information Security Program that outlines Supplier's security policies, practices, and standards.
2. Upon request, Supplier must make the documented Information Security Program available to Ivanti for inspection.
3. When accessing, processing, or otherwise interacting with Ivanti Information Resources, Supplier's personnel must follow Ivanti's Information Security Program, including all Ivanti Policies, Procedures, and Standards.
4. Prior to beginning work, Supplier personnel must review and agree to Ivanti's Acceptable Use Policy.

Authorization and Authentication

1. All accounts, unless explicitly designated as Service Accounts, should be assigned to a named individual who can be held accountable for the actions of the account.
2. Service Accounts should be used sparingly and should be controlled and logged in a way that allows actions performed with the Service Account to be associated with the individual who performed the action.
3. Supplier must have a password policy that indicates requirements for:
    a. Strong password construction according to best practices;
    b. Accounts for the frequency of password changes;
    c. The time permitted before an account is locked for inactivity;
    d. Protects against password reuse and brute forcing, and;
    e. Is available for inspection by Ivanti Information Security upon request.
4. The Supplier must have a documented process or procedure for positively identifying an individual before performing a password reset.
5. The use of PINs is limited to only places where necessary.
6. All non-public resources that are internet facing or all credentials that are considered privileged must use:

a. A secondary hardware or soft-token authenticator that does not utilize SMS in addition to a strong password; or,
b. A certificate-based authenticator that is tied to an individual identity and utilizes industry best practices for certificate generation, handling, and ciphers.

7. In the case that Supplier is provided with Ivanti Accounts, those accounts are assigned to the named individual and may not be shared among other personnel in Ivanti, Supplier, or any other third party.
8. If necessary for the scope of the services provided, Supplier must utilize Ivanti Service Accounts in accordance with Ivanti's applicable policies.
9. Supplier personnel are not permitted to create new or additional Ivanti Accounts or change account permissions of others or themselves unless it is within their defined scope of work.

Physical Security

1. Supplier must ensure that all Information Resources that process, store, transmit, or otherwise interact with Ivanti Data are located in a secure physical facility.
2. Supplier must have a documented process or procedure for secure disposal of data.
    a. The process should include use cases for all media formats that might include Ivanti Data, including digital data stores, physical equipment, and printed content.
    b. The document must be made available to Ivanti Information Security upon request.
3. Supplier must ensure that all physical facilities that contain Information Resources must be protected against common environmental threats.
4. Information Resources that perform production operations for Ivanti must be stored in a designated Data Center.
5. Supplier Data Centers must include physical access controls that log individuals who access the space.
6. Supplier must review physical access to Data Centers, switch closets, and other physical locations that may process, store, transmit, or otherwise interact with Ivanti Data regularly.
7. In the case that Data Center controls are offloaded to a third party (Ex., Colo, Cloud Hosting, etc.), a SOC 2 Type 2 that addresses physical and environment security controls must be made available to the Supplier and reviewed at least annually.

User Workstations

1. If Ivanti is providing workstations to Supplier personnel for the work performed, individuals will be provided a pre-configured system that meets Ivanti's security requirements. In such cases, both Supplier and Supplier personnel must:
    a. Ensure that individuals assigned to Ivanti projects understand that Ivanti will monitor all Ivanti systems, including the Ivanti-provided device, for security and performance proposes;
    b. Ensure that individuals understand it's their responsibility to keep track of the device and take reasonable measures to ensure it does not get stolen or lost.
    c. Ensure access to Ivanti's information resources and data, as well as all tasks, duties, or work performed in support of Ivanti, is performed on the provided device;
    d. Not share, or swap any hardware assigned to them without explicit permission from Ivanti;

e. Not uninstall, disable, circumvent, manipulate the configuration of or otherwise tamper with Endpoint Management, Anti-malware, Host Firewall, Host-based Intrusion Detection Systems (HIDS), or other technology utilized by Ivanti to enforce the security of Ivanti systems without the explicit permission from Ivanti's Information Security Office;
f. Not remove (decrypt), disable, or otherwise tamper with any at-rest encryption (file or full-disk);
g. Not tamper with the configuration of the Ivanti Provided Laptop; and,
h. All Ivanti-provided hardware must be returned to Ivanti within 72 hours of the end of the engagement.

2. If the Supplier is utilizing their own workstations, the Supplier and Supplier personnel must:
    a. User workstations that have access to Ivanti's network, physically or remotely, must have Ivanti Security Tools.
    b. In the case of a conflict between Supplier security/management tools and Ivanti tools, Ivanti tools must take precedence.
    c. Utilize an actively supported operating system that is updated regularly.
    d. Configure the operating system and software according to available best practices and harden it to reduce attack surface (e.g., removing or disabling of superfluous drivers or services, limit unauthorized or unauthenticated user access, etc.).
    e. Be tracked in a centralized asset management system that includes:
        i. A defined owner of the asset
        ii. Details of the hardware and software present
    f. Use an industry-standard full-disk encryption on mobile workstations.
3. The installation of additional software on the Ivanti Information Resources is permitted so long as:
    a. Software licensed and provided by Ivanti is considered first and is preferred over any external software.
    b. Software is installed from a known-good repository.
    c. No additional security tools or system management tools are installed without explicit permission from Ivanti Information Security.
    d. Remote access tools and file share services outside of solutions that are provided and supported by Ivanti are not permitted.
    e. Illegally obtained software (pirated) is not permitted.

Data Protection

1. All Ivanti Data must be encrypted in-transit using industry best-practice encryption methods and key handling. Encryption requirements apply, but are not limited to, all transmissions between Supplier internal information resources, between the Supplier and Ivanti, and any transmission over the internet.
2. All Ivanti Data must be encrypted at-rest using industry best-practice encryption methods and key handling.
3. Data may not be removed from Ivanti systems by any method, including, but not limited to, removable media, cloud services, and email without explicit permission from Ivanti Information Security Team.
4. Removable media, such as flash drives or portable hard drives, may not be used to store Ivanti Data.

5. Supplier must protect Work product (in-progress and final) by appropriately using backup and recovery to ensure recovery can be performed in the case of critical system failure. Ivanti can provide redundant storage locations upon request.
6. All Ivanti sensitive information transmitted through email must be protected by enabling Ivanti-provided email encryption.
7. Ivanti Data should not be accessible to Supplier personnel who are not engaged in providing any services to Ivanti or otherwise do not have a need to know.
8. Sharing Ivanti Data with third parties is prohibited without Ivanti's explicit consent.
9. Ivanti Data may not be used in any way outside of the In-scope Service, including testing functionality/features of the service, without explicit permission from Ivanti Information Security Team.
10. Ivanti Data may not be used as part of any Artificial Intelligence or Machine Learning model without explicit permission from Ivanti Information Security Team.
11. Supplier may not inform any third party that Ivanti is a customer of Supplier without explicit permission of Ivanti.
12. Supplier must have a documented process or procedure for secure disposal of Ivanti Data.
    a. The process should include use cases for all media formats that might include Ivanti Data, including digital data stores, physical equipment, and printed content.
    b. The document must be made available to Ivanti Information Security Team upon request.

Human Resources and Personnel Training

1. Supplier must conduct a background check, where legally permitted, upon hire of Supplier personnel assigned to provide any part of the services to Ivanti or who have access to Ivanti Information Resources or Ivanti Data. The background check must include:
    a. Criminal Background Check
    b. Education Verification Check
    c. Professional Reference Check
    d. Employment Verification
2. Supplier must provide Security Awareness Training, Privacy Training, and any applicable role-specific security training to their employees.
    a. Training should be completed upon hire, prior to performing work, and recertified at least annually thereafter.
    b. Security Awareness Training must include the following topics:
        i. Phishing
        ii. Removable Media
        iii. Physical Security and Clean Desk
        iv. Credential Management
        v. Insider Threats
        vi. Malware
        vii. Incident Reporting
        viii. Data Classification and Handling
    c. Individuals that develop code should receive training on common mistakes that lead to vulnerability (OWASP Top 10, etc.).
    d. Upon request, Supplier must provide training materials to Ivanti Information Security Team or Ivanti's Privacy Team for review.

e. Supplier may opt to take Ivanti Security Awareness and Privacy Training if they do not have a training program or do not meet the above requirements. Training must be completed by Individuals before they begin work.

3. A process for termination or change of status must be documented, enforced, and include notification of such changes to Ivanti for any Supplier personnel that have been assigned to provide any part of the services to Ivanti.
    a. If Supplier provides a SaaS solution to Ivanti, then Supplier is responsible for removing access to Ivanti tenants and Ivanti Data within 24 hours.

Audit and Compliance Requirements

1. Supplier must have controls in place to ensure its compliance with all applicable regulations and laws, including data protection and privacy regulations.
    a. This includes, but is not limited to, compliance with the following Privacy regulations and laws:
        i. California Consumer Privacy Act (CCPA).
        ii. Colorado Privacy Act (CPA).
        iii. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).
        iv. European Union General Data Protection Regulations (GDPR).
        v. UK Data Privacy Act 2018.
    b. This includes compliance with the following regulations:
        i. United States International Traffic in Arms Regulation (ITAR)
2. Supplier must support Ivanti's Vendor Risk Management Process by:
    a. Providing one of the following prior to beginning work, and annually thereafter:
        i. A current, independent SOC 2 Type 2 or ISO 27001 certification; or,
        ii. A completed Ivanti Information Security Team vendor questionnaire.
    b. Responding to all inquiries or requests by Ivanti Information Security Team within ten (10) business days.
    c. Suppliers who are providing engineering contractors for development Work, including development, testing, operations, or support of a product, must have an ISO 27001 or submit to Ivanti Information Security Team additional documentation to show secure development practices.

Security Monitoring and Incident Handling

1. Supplier must have 24/7 monitoring for security events and incidents.
2. In the event of a Data Breach, the Supplier must notify Ivanti Information Security within 72 hours of confirmation to impact of Ivanti Data.
3. In the event that a system that processes or stores Ivanti's Intellectual Property has been accessed by an unauthorized third-party, regardless of whether or not evidence of access to data can be confirmed, Supplier must notify Ivanti Information Security.
4. For any Data Breach or event regarding Ivanti's Intellectual Property, Supplier must support Ivanti by providing applicable logs and evidence so that Ivanti may perform an independent assessment as Ivanti's policies or applicable regulations require.
5. Supplier will provide Ivanti with any details or plans for remediation of any security incident upon request.

Security and Privacy Contacts

The Service Provider must provide points of contact for security and privacy questions and concerns.

Security

Name: _____

Title: _____

Email: _____

Phone: _____

Privacy

Name: _____

Title: _____

Email: _____

Phone: _____

In the event of a security issue, the Service provider will contact Ivanti's Information Security Office via email: security@ivanti.com

In the event of a privacy issue, the Service provider will additionally contact Ivanti Data Protection Officer via email: privacy@ivanti.com

Revision History

Version	Date of Change	Responsible	Summary of Change
1.0	2022/05/26	D. Spicer	Initial version

Date	Reviewed/Approved by
2022/05/26	D. Spicer