Compliance
Third-Party External Vendor Information Security Policy

To establish fundamental security guidelines, requirements, and procedures that reduce risk and provide for the confidentiality, integrity, availability and privacy of Lowe's Companies, Inc., and its subsidiaries ("Lowe's") information technologies and assets. The protection of information assets is mandatory for business, contractual, regulatory, and legal reasons.

A. Scope

This Information Security Policy ("Policy") applies to all Lowe's information technologies and assets, and employees, vendors, contactors, and agents operating on behalf of Lowe's. Individual areas may have additional security and controls, but they are in addition to this Policy. Lowe's reserves the right to amend this Policy at any time.

This Policy is subject to change or termination by Lowe's at any time. Lowe's has full and final discretionary authority for its interpretation and application. This Policy SUPERSEDES all other Policies, Procedures or information conflicting with it.

B. Policy

1. **Information Security Risk Management:** Providers should periodically assess risk within Information Technology specifically toward assets associated with your Lowe's solution(s).

2. **Information Security Policy:** Providers should document their Information Security Policies and follow Information Security programs that are based on at least one of the following frameworks:
    - International Organization for Standardization (ISO) 27002,
    - Information Security Forum (ISF) Standards of Good Practice (SoFP)
    - ISACA Control Objectives for Information and Related Technologies (COBIT), or
    - National Institute of Standards and Technology (NIST) Special Security Publications.

    Providers should map their security program to one of the above security frameworks showing no gaps in their information security program.

3. **Organization of Information Security**
    - Providers should define, document, and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards, and procedures.
    - Providers should ensure the assigned role should be of a sufficiently high-level classification in the organization that can be allowed to execute the responsibilities in an effective and independent manner.

    Note: To avoid conflicts of interest, providers should ensure this role will not have direct responsibility for information processing and technology operations.

4. **Inventory and Control of Enterprise Assets Management**
    - Provider should establish a process to actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) that connects to the providers infrastructures physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise.
    - Providers must have a managed and up-to-date inventory of Providers Assets that access Lowe's assets and data.
    - Provider should assign designated individual that is responsible for all Provider Assets that access Lowe's assets and data
    - Review and update asset inventory on at least annual basis.

5. **Inventory and Control of Software Assets**
    - Providers must actively keep inventory, track, and manage all software on the provider's network to ensure that only authorized software is installed on operating systems and applications that access Lowe's data.
    - Ensure any unauthorized software is removed from enterprise assets or receives a documented exception
    - Ensure only authorized software can be executed or accessed.
    - Ensure only authorized software libraries are allowed to load into a system process

6. **Data Protection**

   Provider should:

   Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

   - Establish a data classification policy, maintain data inventory and segments data processing and storage based on the sensitivity of the data.
   - Encrypt all Lowe's data assets in transit between provider and Lowe's and any transmission of Lowe's data between provider and all other third parties with a minimum of TLS 1.2.
   - Encrypt regulated/sensitive information "at rest" on servers, applications, and databases within the provider's facility or at the hosting provider with a minimal standard of AES-256-bit encryption.
   - Encrypt all end-user devices containing sensitive data
   - All laptops should have full hard disk encryption.
   - Encrypt data on all removable media.
   - Use strong encryption key management practices to ensure the availability of encrypted authoritative information
   - Provider should sign and encrypt API requests.
   - Provider should encrypt data at rest and in transit in accordance with all regulatory bodies (e.g., PCI), local and national laws (examples are, but are not limited to the following: HIPPA, SOX, GLBA, etc.).
   - Providers should secure all Credit Card data per the requirements listed in the most current and released editions of the Payment Card Industry – Data Security Standards (PCI-DSS).

7. **Secure Configuration of Enterprise Assets and Software**

   - Provider should establish and maintain a secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
   - Implements and manages a firewall on servers and end-user devices
   - Uninstall or disable unnecessary services on enterprise assets and software.
   - Enforce Automatic Device Lockout on Portable End-User Devices
   - Enforce Remote Wipe Capability on Portable End-User Devices

8. **Account Management**

   Provider should use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

   - Establishes and maintains an inventory of all accounts used to access Lowe's data
   - Establish strong password policy procedure and enforce the use of unique IDs for all accounts that access Lowe's data or asset
   - Ensure administrator privileges are restricted to dedicated administrator accounts
   - Do Not allow Lowe's or provider employees or subcontractors direct root access to any systems or access to the administrator user account.
   - Disable or delete dormant user account.

9. **Access Control Management**

   Providers should:

   - Establish a policy and process to create, assign, manage, and revoke access credentials and privileges for a user, administrator, and service accounts for enterprise assets and software.
   - Develop and implement processes for ensuring adequate authentication and authorization for all employees, contractors, and subcontractors with access to the Company assets.
   - System access authorization should be based on business requirements whiles enforcing the principle of least privileges and Need-to-know.
   - Ensure password policies and standards exist on IT systems that access Lowe's assets.
   - Ensure controls restrict other provider customers from accessing Lowe's assets.
   - Ensure IT administrators are provided and use separate and unique administrator accounts only for administrative responsibilities. Non-administrator tasks should always be performed using non-administrator user accounts.
   - Provider must enforce multi-factor authentication (MFA) for
     - Privileged administrative access to applications, systems and databases that process, transmit or stores Lowe's data.
     - Access to network routers, switches, and load balancers; access to network services (DNS, NTP, etc.); any interactive shell or admin access to systems in internet-facing DMZs.
   - Provider should enforce centralize access control for all enterprise assets through a directory service or SSO provider.

- Providers should ensure systems that access Lowe's assets always meet the following additional requirements:
  - *Authentication credentials should be encrypted when stored or transmitted at all times*
  - *Providers must not share password for user-level accounts between multiple individuals. Passwords for individual user accounts should never be given to or shared with someone other than the account owner.*
  - *Providers should change passwords immediately whenever an account is suspected to be compromised.*
  - *Passwords should not be communicated via email messages or other forms of electronic communications, other than one-time use passwords.*
  - *Provider should verify a user's identity before password reset and send a notification email or voicemail to the user regarding the password reset.*
  - *Set first-time passwords for new user accounts using unique values that are not generic or easily guessed and follow the requirements outlined in this policy.*
  - *Configure user accounts to force a change of password upon first use of a new account or after a password is reset.*
  - *All manufacturer passwords should be changed from their default values (including when the default value is NULL) and should meet the requirements set forth in this policy. Manufacturer passwords include, but are not limited to, SNMP community strings, system-level administrator account passwords, temporary account passwords, wireless encryption keys, and other default authentication settings.*
  - *Do not use Production account passwords in non-production environments.*
  - *If a system-level administrator account (e.g., Windows local administrator or UNIX/Linux root) is used to perform privileged management of a device, that password should be changed following completion of that management task.*
  - *System-level account passwords should be unique on each device.*
  - *All systems should prompt users to re-0authenticate when users attempt to elevate their privileges to higher security levels. Examples include use of sudo or su on UNIX/LINUX systems or "run as" for Microsoft Windows based systems.*

Note: Provider should not install technology that provides remote access to any asset on the Lowe's network including, but not limited to analog phone line remote access technologies (e.g., modems), Virtual Private Networks, Remote access software, etc.

10. **Human Resources Security**

Providers should:

- Ensure all provider employees, contractors, and subcontractors who access Lowe's assets and Regulated, Confidential or Personal Information are screened/vetted prior to employment. Screening should include criminal and employment background screening processes.
- Provider employees, contractors, and subcontractors should agree to and sign a Non-Disclosure Agreement (NDA) and compliance with the organizational security policies prior to starting their work, including access to Lowe's data or assets.
- Immediately notify Lowe's in writing if a provider employee or subcontractor is no longer working on Lowe's account or should change ID permission on Lowe's managed assets and data. Notices should include the employee's name and user ID of any accounts the employee had access to or knows the account password.
- Upon employee termination or exit, Provider's HR Department should ensure that all equipment or assets with Lowe's data assigned to the external employee or subcontractor are returned to the company before the employee leaves.

11. **Security Awareness and Skills Training**

- Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and ensure compliance with security policies.
- Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Include role-based training to ensure employees receive the required training relevant to their job role
- Ensure all employees and contractors who have access to Lowe's assets complete annual security awareness training.

12. **Continuous Vulnerability Management**

- Providers must establish and maintain documented vulnerability management program that specifies the approach to continuously assessing and tracking system and application vulnerabilities. The policy and procedure document should be reviewed at least annually.
- Conduct periodic vulnerability assessments on infrastructure, network, and applications vulnerability scans following industry-acceptable vulnerability management practices (e.g., the process described in NIST & OWASP)
- Perform network and application vulnerability scans a monthly or more frequent basis.

- Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- Providers must provide Lowe's with the **latest network and application vulnerability scan report.**

13. **Audit Log Management**

    Providers must implement a process to collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

    - Establish and maintain an Audit Log Management Process.
    - Maintain DNS query logs, event logs, and security logs
    - Ensure access and activity audit and logging procedures exist, including access attempts and privileged access.
    - Retain audit all audit logs for a minimum of 90 days and enforce processes to ensure that audit logs are not modified.
    - Periodically reviews audit logs to detect anomalies and potential threats

14. **Email and Web Browser Protections**

    Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

    - Ensure the use of Only Fully Supported Browsers and Email Clients
    - Enforces and updates network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites.
    - Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.
    - Deploy and Maintain Email Server Anti-Malware Protections such as attachment scanning and/or sandboxing.

15. **Malware Defenses**

    The provider should ensure a malware protection solution is deployed on all IT systems that access Lowe's assets and data.

    - Deploy and Maintain Anti-Malware Software on all enterprise assets.
    - Provider shall prevent or control the installation, spread, and execution of malicious applications, code, scripts, or creation of backdoor on enterprise assets.
    - Provider should ensure Malware Protection technology has the latest and up-to-date manufacture’s signatures, definition files, software, and patches.

16. **Data Recovery**

    Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

    - Establish and maintain a data recovery process
    - Perform automated backups for all Lowe's data.
    - Test backup recovery at least quarterly.

17. **Network Infrastructure Management**

    Establish, implement, and actively manage (track, report, correct) network devices to prevent attackers from exploiting vulnerable network services and access points.

    - Securely manage the network infrastructure and enforce security Authentication, Authorization, and Auditing.
    - Establish and Maintain a Secure Network Architecture and provide a dataflow diagram upon request to Lowe's.
    - Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).
    - Enforce VPN connections for all remote devices connecting to an Enterprise's.

18. **Network Monitoring and Defense**

    Operate processes and tools to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise’s network infrastructure and user base.

    - Providers should deploy network and host-based monitoring solution (Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)) at perimeter points where Lowe’s regulated, confidential or personal information is used.
    - Providers should ensure all unnecessary services, ports, and network traffic are disabled on all IT systems that access Lowe’s assets.
    - Perform traffic filtering between network segments, where appropriate.
    - Providers should ensure that Web Server, Application Servers, and database administrative functions are only accessed via SSH or a secure method that encrypts traffic during transmission.

19. **Service Provider Management**
    - Providers should create an effective third-party/vendor policy which includes steps to ensure compliance with applicable laws, regulations, and best practices. Ensure that the vendor policy is reviewed and updated annually.
    - Providers should evaluate service third-party/vendors who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes to ensure these providers are protecting those platforms and data appropriately.

20. **Application Software Security**

    Providers should manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they impact the enterprise.
    - Establish and maintains a secure application development process
    - Ensure industry acceptable application development security standards (e.g., OWASP) are followed so that IT systems and applications are tested and secured in every step of the application and system development life cycle.
    - Maintain separate environments for production and non-production systems.
    - Ensure firmware, software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.
    - Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.
    - Properly manage application vulnerabilities identified during development and testing and perform root cause analysis.

21. **Mobile Device Management (MDM) Policy**

    Establish an effective MDM policy where all mobile devices, whether owned by The Company or owned by employees, inclusive of smartphones and tablet computers, that have access to corporate networks, data, email, and systems are governed by this mobile device security policy.
    - Enforce full-disk encryption on all mobile devices used to access Lowe’s data.
    - Enforce strong authentication to prevent unauthorized access
    - Enable remote wipe capabilities on all mobile devices

22. **Removable Media/Offsite Storage Policy**

    Provider should ensure that devices are not allowed to save records on removable media. If necessary, company USB devices with mandatory encryption will be used. Data stored offsite (including backups and cloud storage) requires encryption of data at rest.

23. **Incident Response Management**

Providers should

- Develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack
- Ensure security incident response planning and notification procedures exist to monitor, react, notify, and investigate any incident related to Lowe's assets.
- Immediately notify Lowe's if provider identifies a breach in any controls that impacts a Lowe's asset or data related to a Lowe's asset.
- **Incident Reporting:** All Third-Party Vendors are contractually required to report the following security issues as it relates to Lowe's Data:
    - Security violations,
    - Breaches within areas where Lowe's data is present.
    - Send report Lowe's via email to (soc@lowes.com).

  Note: Once provider(s) discover or are notified of a security breach, provider should investigate, fix, restore and conduct a root cause analysis.
- Provide Lowe's with results and frequent status updates of any investigation related to Lowe's. Please send emails to soc@lowes.com.
- If Lowe's is not satisfied with speed or effectiveness of investigation, provider(s) should include Lowe's Information Security staff in the investigation and response teams.

24. **Penetration Testing**

Providers must test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology) and simulating the objectives and actions of an attacker.

- Conduct **annual penetration test** utilizing third-party or independent resources.
- Establish remediation policy and ensure that penetration test findings are remediated according to the established timeframes.
- Providers must the provide **latest annual penetration test** conducted by an independent third-party or internal personnel.
- Lowe's does not need specific issues found during either test. An executive summary indicating the number of critical/high, medium, and low issues found is required. Evidence of remediation required.

25. **Business Continuity Management**
    - Establish and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures document at least annually.
    - Test business contingency plan at least annually to ensure operational effectiveness
    - Designate roles and responsibilities for managing business contingency plans.

26. **Disaster Response Plan**
    - Establish and maintain a disaster response plan to resolve data loss and recover system functionality following an incident. Update the plan at least annually or upon significant changes.
    - Test the operational effectiveness of the disaster recovery plan at least annually.
    - Designate roles and responsibilities for managing disaster recovery plans

27. **Physical and Environmental Security:**

    Provider should store Lowe's assets in locations that are protected from:
    - Natural disasters
    - Theft, physical intrusion, unlawful and unauthorized physical access
    - Ventilation, Heat or Cooling problems, power failures or outages

28. **Offshore Locations:** If data is located outside of the United States, please follow the "Clean Room" concept. Ensure that policies, standards, and guidelines for all aspects prevent data exfiltration.

29. **External Audits and Certification**
    - Providers must provide an independent audit report (preferrable SOC 2 Type II report, ISO27001 Certification
    - Providers accessing credit card data should provide evidence of PCI certification/compliance and the Roles and Responsibilities Matrix annually.

30. **Additional Requirements for Hosting Service Providers**

In addition to all requirements listed in all prior sections, all providers who provide hosting services to Lowe's should follow the following requirements. Hosted services include, without limitation, cloud computing or offsite hosting services. Cloud computing can be provider service offerings that allow Lowe's to lease dynamically and provision infrastructure, virtual environments, platforms, and software.

- Providers that provide hosting services are responsible for all requirements below. In event, the provider's hosting service model shifts some responsibility of the below requirements to Lowe's, the provider should still complete a "Policy Exception Request" as defined in the "Filing for a Policy" Section of this document to clearly define ownership or responsibility. Lowe's will not assume any ownership for any requirement below without a direct agreement listed in a written contract, statement of work, or a Lowe's approved Policy Exception Request.
- Providers who provide infrastructure and platform hosting services should ensure non-Lowe's authorized personnel cannot physically or electronically inspect, insert, share, access, steal or change the content of Lowe's assets, including without limitation Lowe's used network, traffic, infrastructure, applications, RAM, and storage space.
- Providers should ensure Lowe's assets reside on separate physical hardware from other service provider customers, including data distributed in different environments (e.g., backup media, production, development, test quality assurance, disaster recovery) when transferring or storing Lowe's Regulated, Personal, or Confidential Information.
- Providers should ensure that all mappings to the objects or domains are removed when objects and domains are deleted.

31. **Remediation**

Providers will work with third-party risk analysts if they do meet a minimum standard. The analyst will document any occurrence as a finding, this finding will be shared with vendor contact, a plan will be provided to mitigate the risk or remediate, and this information will be documented.

32. **Non-Compliance**

Failure to comply with any part of these Information Security requirements, is covered within the contract between Lowe's and the Third-Party Vendor.