Information Security Group (ISG) Global	**Third-Party External Vendor Requirements**	
	Governing Policy: POL-ISG-2.0 Security Risk Management	**Effective Date: 3/24/2017**

1. Purpose

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.

2. Scope

This Information Security Policy ("Policy") applies to all Lowe's information technologies and assets, and employees, vendors and agents operating on behalf of Lowe's using the aforementioned. 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.

3. Policy

3.1 Requirements for all Third Parties

3.1.1 Information Security Risk Management

Providers should periodically assess risk within Information Technology specifically toward assets associated with your Lowe's solution(s).

3.1.2 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), 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.

3.1.3 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, you should ensure this role will not have direct responsibility for information processing and technology operations.

3.1.4 Asset Management

Providers should 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.

Providers should document and implement rules for the acceptable use of assets of third parties, including without limitation, Lowe's assets and data.

- Rules of acceptable use should require that third party assets are not be used for activities which have been identified as unacceptable conduct.
- Rules of acceptable use should require that third party assets are to be used in a professional, lawful and ethical manner.

All providers who connect to or use a Lowe's asset (including servers, workstations, infrastructure, internet gateway or network) should abide by all applicable Lowe's terms of use, policies, standards, and procedures. Companies are required to safeguard and use Lowe's assets wisely and will use good judgment and discretion when using Lowe's assets including Lowe's systems, computers, telephones, internet access, email, voice mail, copiers, fax machines, vehicles or other property.

Providers should never connect non-Lowe's owned assets to the provider network without direct written approval from Lowe's.

- Lowe's should review and approve all requests from any company to connect non-Lowe's owned assets to the Lowe's network.
- Assets that connect to Lowe's network should abide by Lowe's security Policies, Standards, Operating practices and controls, including, but not limited to configuration, hardening, patching, access control and virus protection processes.

3.1.5 Human Resources Security

Providers should:

- Ensure all provider employees, contractors, and subcontractors who access Lowe's assets are screened prior to employment. Screening should include criminal, financial, employment background screening processes.
- Have processes in place to periodically screen personnel during employment for anyone who accesses Regulated, Confidential, or Personal information.
- Ensure an Information Security awareness campaign is provided to everyone who has access to Lowe's assets. Campaign should educate personnel of their responsibility to secure Lowe's assets.
- Ensure all user IDs, tokens or physical-access badges are assigned to a unique provider employee or provider subcontractor.
- Ensure all user/system/service/administrator accounts and passwords are never shared.
- Immediately notify Lowe's in writing if a provider employee or subcontractor is not working on the Lowe's account or ID permission should be changed on a Lowe's managed assets and data. Notices should include name, user ID name of any accounts the person had access to or knows the password.

3.1.6 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.

3.1.7 Operations Management

3.1.7.1 Network Security

Providers should deploy Data Loss Prevention (DLP) and or intrusion monitoring services 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.

3.1.7.2 System Security

Providers should have a process for applying and managing security updates, patches, fixes upgrades, (collectively referred to as "Patches") on all provider IT systems.

Provider should ensure Malware, Virus, Trojan and Spyware protection is deployed on all IT systems that access Lowe's assets and data.

Provider should ensure Malware, Virus, Trojan and Spyware protection technology have the latest and up-to-date manufacture's signatures, definition files, software and patches.

Provider should deploy methods to identify malicious activity, log information such activity, attempt to block/stop the activity, and to report such activity.

- Security methods should have the latest and up-to-date manufacture's signatures, definition files, software patches.
- If requested by Lowe's, provider should supply logging information of all unauthorized activity going back a minimum of one year.

Providers should ensure all unused or unnecessary software, applications, services, sample/default files and folders are disabled on all IT systems that access Lowe's assets and data.

3.1.7.3 Data Security

Provider should:

- Use strong encryption key management practices to ensure the availability of encrypted authoritative information
- Encrypt all Lowe's data assets in transmission between provider and Lowe's as well as between provider and all other third parties when transmitted data is Lowe's data.
- Encrypt regulated information when it is "at rest" at all times.
- Encryption should meet a minimal standard of AES-256-bit encryption.

3.1.7.4 Operation Security

Providers should:

- Ensure that any changes to IT systems that are performing work on or for Lowe's do not have any negative security implications.
- Follow documented change management practices and procedures
- Not move or transfer Regulated, Personal or Confidential information to any non-production environment or insecure location.

3.1.8 Access Control

Providers should:

- Ensure controls restrict other provider customers from accessing Lowe's assets.
- Use authentication and authorization technologies for service, user and administrator level accounts.
- Not allow Lowe's or provider employees or subcontractors direct root access to any systems or access to the administrator user account.
  Note: For Unix or Unix-like operating systems, users should use the "sudo" command where all access should be logged.

- Ensure IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administrator tasks should always be performed using non-administrator user accounts.
- Ensure password policies and standards exist on IT systems that access Lowe's assets
- Providers should ensure systems that access Lowe's assets meet the following additional requirements at all times:
  - *Authentication credentials should be encrypted when stored or transmitted at all times*
  - *Passwords for user-level accounts cannot be shared between multiple individuals*
  - *Providers should change passwords immediately whenever it is believed that an account may have been compromised.*
  - *Passwords should not be communicated via email messages or other forms of electronic communications, other than one-time use passwords.*
  - *Passwords for individual user accounts should never be given to or shared with someone other than the account owner*
  - *A user's identity should be verified before their password is reset and email or voicemail notification should be sent to notify the user that their password was reset.*
  - *First time passwords for new user accounts should be set to unique values that follow the requirements set forth in this policy and should not be generic, easily-guessed passwords.*
  - *User accounts should be configured to force a change of their 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.*
  - *Password fields should display only masked characters as the user types in their password, where technically feasible.*
  - *Hardcode plain-text passwords should not be used in production environments.*
  - *Production account passwords should not be used 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.*
- *If an account has machine-set complex password of 20 characters or more that is never accessed or known by a person, that passwords does not need to be changed during its lifetime, unless the account or its associated system has been suspected of compromise.*
- *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.*

- Providers should ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.
- Providers should ensure procedures exist for provisioning privileged accounts.
- Providers should periodically review the necessity of privileged access accounts
- If provider requires remote access to Lowe's assets, providers should always use a Lowe's approved method to remotely connect to any Lowe's asset.

  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.

3.1.9 Information Technology Acquisition, Development and Maintenance

Providers should:

- Ensure infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices (e.g. process described in NIST & OWASP)
- 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.
- Ensure firmware, software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.

3.1.10 Information Security Incident Management

Providers should:

- Ensure access and activity audit and logging procedures, including access attempts and privileged access, exist.
- 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.

  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 update of any investigation related to Lowe's.

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.

3.1.11 Compliance

- Data destruction processes should follow a process that securely wipes all data on all media using a method that will not allow data to be retrieved. For all IT systems that access Regulated, Confidential, or Personal Information, Lowe's requires the destruction be performed in accordance with NIST Special report 800-88, Gutmann Method, US DoD 5220-22.M
- If requested by Lowes, provider should provide adequate validation of any subcontracted company is compliant with this policy.
- Provider should obtain written permission from the Lowe's legal department to move
- Providers should secure all Credit Card data in accordance to requirements listed in the most current and release editions of the Payment Card Industry – Data Security Standards (PCI-DSS or PCI).
- Providers that access credit card data should annually provide evidence of PCI certification/compliance.

3.2 Additional Requirements for Hosting Service Providers

In addition to all requirements listed in all prior sections, the following requirements should be followed by all providers who provide hosting services to Lowe's. Hosted services include, without limitation, cloud computing or offsite hosting services. Cloud computing can be provider service offerings that allow Lowe's to dynamically lease 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 "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.

3.2.1 Operations Management

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 content of Lowe's assets, including without limitation Lowe's used network, traffic, infrastructure, applications, RAM and storage space.

3.2.1.1 Network Security

Within Lowe's used or leased services, providers should restrict by protocol , service port and source IP address, and MAC address through the use of firewall technologies.

Providers should ensure firewalls are configured with different policies that allow Lowe's used web servers, application servers and databases are protected with different levels of security.

- Providers should ensure network segmentation and firewall restrictions exist so that Lowe's used database servers can only communicate with the following:
  - Application servers located in an application Virtual Local Area Network (VLANs)
  - Management tool servers located in Management Tool VLANs
  - Network Administration users located in Admin VLANs.
- Providers should ensure network segmentation and firewall restrictions exist so that Lowe's used application servers commonly communicate with the following:
  - Web servers located in the Web VLANs,
  - Databases located in database VLANs,
  - Management tool servers located in management tool VLANs,
  - Network administration users located in Administration VLANs.
- Providers should use additional security protection controls for protecting against access to Lowe's Regulated, Personal, or Confidential information, such as:
  - Web application firewalls,
  - Intrusion detection systems,
  - Intrusion prevention systems,
  - Data loss prevention systems.
- Providers should ensure Web Server, Application Servers, and database administrative functions are only accessed via SSH or a secure method that encrypts traffic during transmission.

3.2.1.2 System Security

Providers should ensure Lowe's assets reside on a 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.

For services that leverage Virtual Environments (VE), providers should ensure VE's:

- Use Lowe's standard builds or Lowe's approved builds,
- Provider provided platform, build, standard image, or related template for guest operating systems, are validated by Lowe's to ensure security requirements are correctly integrated.
- OS patches are easily deployable to all un-patched servers and applications so that all servers can comply with Lowe's patch management standards.
- VE specific security mechanisms embedded in hyper vision APIs are utilized to provide granular monitoring of traffic crossing VE backplanes, which will be opaque to traditional network security controls.
- Administrative access and control of VE operating systems include strong authentication integrated with enterprise identity management, as well as tamper-proof logging and integrity monitoring tools.
- Are segregated in security zones by type of usage (e.g., desktop vs server), production stage (e.g., development, production and testing) and sensitivity of data (e.g. Lowe's Regulated data) on separate physical hardware components such as servers, storage, etc.
- Have a reporting mechanism in place that provides evidence of VE isolation and raises alerts if there is a breach of isolation.
- Have capability for File Integrity Monitoring (FIM) to be deployed on VEs to alert on critical file changes.

Providers should configure and filter inbound and outbound traffic per instance using host-based firewalls.

3.2.1.3 Data Security

Provider should encrypt data at rest and in transit in accordance to all regulatory bodies (e.g., PCI), local and national laws (examples are, but are not limited to the following; HIPPA, SOX, GLBA, etc).

Provider should sign and encrypt API requests.

3.2.1.4 Operations Security

Provider should ensure:

- That when objects are deleted, all mappings to the objects are also removed.
- That when domains, objects and trusts are deleted, all mappings to the domains, objects and trusts are also removed.
- Provider should provide Lowe's with the ability to monitor and review critical files for changes or tampering.

3.2.2 Access Control

For systems that access Lowe's classified Confidential, Personal or Regulated information, provider should deploy and offer token or key-based authentication to improved authentication controls.

4. Incident Reporting

All Third Party Vendors are contractually required to report the following security issues as it relates to Lowe's Data:

- Potential security threats observed,
- Security violations,
- Breaches within areas where Lowe's data is present.

Report must be sent to Lowe's, via email to (soc@lowes.com).

5. 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.