Information Security Group (ISG)	**Information Technology (IT) Third Party - Policy**	
	Policy Number: POL-004-300 Version 4.0	**Effective Date: 7/11/2014**

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

3.1.2 Information Security Policy

Providers must 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 must 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 must define, document, and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards, and procedures.

Providers must ensure the assigned role must 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 must ensure this role will not have direct responsibility for information processing and technology operations.

3.1.4 Asset Management

Providers must have a managed and up-to-date inventory of Providers Assets that access Lowe's assets and data.

Provider must assign designated individual that is responsible for all Provider Assets that access Lowe's assets and data.

Providers must 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 must require that third party assets are not be used for activities which have been identified as unacceptable conduct.
- Rules of acceptable use must 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) must 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 must never connect non-Lowe's owned assets to the provider network without direct written approval from Lowe's.

- Lowe's must 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 must 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 must:

- Ensure all provider employees, contractors, and subcontractors who access Lowe's assets are screened prior to employment. Screening must 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 must 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 must be changed on a Lowe's managed assets and data. Notices must 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 must 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 must deploy Data Loss Prevention (DLP) and or intrusion monitoring services at perimeter points where Lowe's regulated, confidential or personal information is used.

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

- Providers must ensure patches that provide security fixes or security updates are deployed within 30-days from the date of release, for Lowe's IT systems that access Confidential, Personal, or Regulated Information.
- Otherwise, providers must ensure patches are deployed within 120-days from the date of release.

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

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

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

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

Providers must 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 must:

- 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 must meet a minimal standard of AES-256-bit encryption.

3.1.7.4 ***Operation Security***

Providers must:

- 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 must:

- 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 must use the "sudo" command where all access must be logged.
- Ensure IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administrator tasks must always be performed using non-administrator user accounts.
- Ensure password policies and standards exist on IT systems that access Lowe's assets
- Ensure systems that access confidential, personal or regulated information require the following password construction requirements at all times:

  i. *Minimum length of 8 characters for accounts other than administrative or elevated accounts (Local Admin, Domain Admin, root, etc.). Administrative or elevated accounts require a minimum of 15 characters.*

  ii. *Complexity must contain at least three of the following four characters (Number, Uppercase Letter, Lowercase letter, Printable special character)*

  iii. *When changing or rotating an account password, the reuse of any of the prior 10 passwords is not allowed*

  iv. *Account password expiration (the requirement to change and existing account password), must occur at - or less than 90 days.*

  Note: This applies to all accounts including administrative and service/application accounts.

  v. Service accounts must be changed at – or less than 90 days.

  vi. Failed login attempts, when exceeding 6 consecutive attempts, must lock the account.

  vii. When and account is locked due to 6 failed login attempts, the account must remained locked for a minimum of 30 minutes.

  viii. Screen saver locks must be enabled to lock access after 15 minutes of keyboard inactivity.
- Providers must ensure systems that access Lowe's assets meet the following additional requirements at all times:

  i. Authentication credentials must be encrypted when stored or transmitted at all times

  ii. Passwords for user-level accounts cannot be shared between multiple individuals

iii. Providers must change passwords immediately whenever it is believed that an account may have been compromised.

iv. Passwords must not be communicated via email messages or other forms of electronic communications, other than one-time use passwords.

v. Passwords for individual user accounts must never be given to or shared with someone other than the account owner

vi. A user's identity must be verified before their password is reset and email or voicemail notification must be sent to notify the user that their password was reset.

vii. First time passwords for new user accounts must be set to unique values that follow the requirements set forth in this policy and must not be generic, easily-guessed passwords.

viii. User accounts must be configured to force a change of their password upon first use of a new account or after a password is reset.

ix. All manufacturer passwords must be changed from their default values (including when the default value is NULL) and must 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.

x. Password fields must display only masked characters as the user types in their password, where technically feasible.

xi. Hardcode plain-text passwords must not be used in production environments.

xii. Production account passwords must not be used in non-production environments.

xiii. 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 must be changed following completion of that management task.

xiv. 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.

xv. System-level account passwords must be unique on each device.

xvi. All systems must 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 must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.
- Providers must ensure procedures exist for provisioning privileged accounts.
- Providers must periodically review the necessity of privileged access accounts

- If provider requires remote access to Lowe's assets, providers must always use a Lowe's approved method to remotely connect to any Lowe's asset.

  Note: Provider must 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 must:

- 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 must:

- 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 must 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) must include Lowe's Information Security staff in the investigation and response teams.

3.1.11 Compliance

- Data destruction processes must 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 must provide adequate validation of any subcontracted company is compliant with this policy.
- Provider must obtain written permission from the Lowe's legal department to move Lowe's assets across any international borders.

- Providers must 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 must 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 must 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 must 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 must 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 must restrict by protocol , service port and source IP address, and MAC address through the use of firewall technologies.

Providers must 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 must ensure network segmentation and firewall restrictions exist so that Lowe's used database servers can only communicate with the following:
    a) Application servers located in an application Virtual Local Area Network (VLANs)
    b) Management tool servers located in Management Tool VLANs
    c) Network Administration users located in Admin VLANs.

- Providers must ensure network segmentation and firewall restrictions exist so that Lowe's used application servers commonly communicate with the following:
    a) Web servers located in the Web VLANs,
    b) Databases located in database VLANs,
    c) Management tool servers located in management tool VLANs,
    d) Network administration users located in Administration VLANs.
- Providers must use additional security protection controls for protecting against access to Lowe's Regulated, Personal, or Confidential information, such as:
    a) Web application firewalls,
    b) Intrusion detection systems,
    c) Intrusion prevention systems,
    d) Data loss prevention systems.
- Providers must 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 must 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 must 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 must configure and filter inbound and outbound traffic per instance using host-based firewalls.

3.2.1.3 ***Data Security:***

Provider must 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 must sign and encrypt API requests.

3.2.1.4 ***Operations Security:***

Provider must 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 must 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 must deploy and offer token or key-based authentication to improved authentication controls.

4. Maintenance

All change requests to the information security policies must be submitted in writing to the Information Security Group. If necessary, the Information Security Management Committee will review such change requests. The Information Security Management Committee is responsible for approving all updated information security policies.

5. Custodian

The custodian of this policy is the Vice President of Information Security. The Vice President of Information Security is responsible for implementation of all security policies. Any questions regarding the implementation of this policy should be directed to the Vice President of Information Security.

6. Sponsor

The sponsor of this Policy is the Chief Information Officer (CIO). The Vice President of Information Security is responsible for the implementation and assurance of this Policy. Any questions regarding the implementation of this Policy shall be directed to the Vice President of Information Security. The Vice President of Information Security is responsible for any policy exceptions and waivers related to this Policy. The sponsor and custodian must jointly approve any additions, deletions or modifications to this Standard.

7. Incident Reporting

All users are required to report potential security threats or security violations directly to their direct management and ISG.

All users may report any inappropriate use of Lowe's IT assets directly to ISG Management or through the "LOWES OPEN DOOR SERVICE" (1-800-784-9592) for investigation and possible disciplinary action.

8. Compliance

Failure to comply with any part of this policy or any related information technology security policy, procedure or standard may result in disciplinary action up to and including termination of employment, services or relationship with Lowe's as well as action in accordance with state laws, federal laws, or international laws, regarding computer crimes.

Any action to compromise security measures without specific advance approval from the Information Security Group, including but not limited to system or password cracking/guessing, reverse engineering of software, file decryption, or improper software licensing or copying, or use of techniques to gain logical or physical access without authorization is a violation of this policy and considered an offense.

Any unlawful act of Lowe's IT systems is a critical offense and will result in Lowe's turning the offender(s) and any/all evidence of unlawful activity over to the appropriate authorities. All users may report any inappropriate use of Lowe's IT assets directly to the ISG Management or through the Ethics Help Line (1- 800-784-9592) for investigation and possible disciplinary action.

Non-compliance to the criteria specified in this policy must be approved via the Lowe's Exception – Waiver submission process.

9. Filing for a waiver exception

Information security policy exception requests must be submitted in writing to Vice President or Director of Information Security, including justification and benefits attributed to such exceptions. The Information Security Group is responsible to review and make recommendations on procedural or technical alternatives that enable policy compliance. Waivers should only be used in exceptional situations and will be limited to a specific period of time. The status of all waivers approved or not, will be reported to the ISMC.