



## **Information Security Policy**

### **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 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 Information Security Policy ("Policy") at any time.

### **3. Policy**

#### **3.1. General Requirements**

To provide for the confidentiality, integrity, availability and privacy of information assets, Lowe's must prevent the unauthorized modification of and access to such.

Lowe's information technologies store and process a wide array of sensitive information including, but not limited to, employee personnel data, customer credit cards, financial data and strategic plans. See *Lowe's Code of Business Conduct and Ethics*.

The use of computer software is regulated by State and Federal Copyright laws. The use of any computer software not specifically authorized by vendor agreements and Lowe's management is prohibited, and subject to disciplinary action and prosecution under State and Federal laws. Employees with information or knowledge of computer software being used in a prohibited manner must immediately report such matters to their management or Internal Audit.

#### **3.2. User Requirements**

Individuals must exercise responsible, ethical behavior when using Lowe's information technologies. Additionally, the following applies:

- 3.2.1. Compliance with all Lowe's security policies is mandatory, including but not limited to *User Account, Internet Abuse, Email Security, Network Security, Remote User, Internet/Intranet Firewall and Non-Lowe's Device Connectivity*.
- 3.2.2. All users, in consideration for being permitted access to Lowe's information technologies, applications and company-sensitive information, are accountable for their protection and proper use.
- 3.2.3. Access to Lowe's information technologies and assets is only provided management approved users.
- 3.2.4. Unauthorized or inappropriate use of Lowe's information technologies and assets is strictly prohibited.

- 3.2.5. It is strictly prohibited to use another employee's logon ID, or to provide false or misleading information to obtaining access to Lowe's information technologies and assets.
- 3.2.6. Users of Lowe's information technologies and assets must regularly change passwords (which are considered confidential).
- 3.2.7. Users must take all necessary precautions to protect Lowe's information technologies and assets, their own programs and programs residing in software libraries.
- 3.2.8. Users are responsible for the proper handling, storage and disposal of any media produced through Lowe's information technologies including but not limited to diskettes, tapes, paper copies, E-mails, microfiche and compact disks.
- 3.2.9. The use of Lowe's information technologies and assets other than for conducting Lowe's business is strictly prohibited.
- 3.2.10. The tampering with or changing the configurations of Lowe's information technologies and assets is strictly prohibited.
- 3.2.11. Executing programs of unknown origin is strictly prohibited.
- 3.2.12. Users must take the necessary precautions to lock terminals or logout if the terminal is left unattended.
- 3.2.13. Shared common information identified as sensitive, confidential or otherwise proprietary (see *Lowe's Code of Business Conduct and Ethics*) may only be stored on approved corporate servers.

### **3.3.Maintenance, Management and Monitoring of User Accounts**

To protect the confidentiality, integrity, availability and privacy of Lowe's information technologies and assets, Lowe's reserves the right to:

- Limit, restrict, or terminate any or all access by a user. This includes terminating any unused logon ID after 90 days with or without prior notice.
- Inspect, copy, or remove any file or system resources that may undermine the authorized use of that Lowe's information technology or asset, with or without prior notice.
- Routinely check Lowe's information technologies and assets, and take all necessary actions to protect such, as there is no expectation of privacy while using Lowe's information technologies.
- Monitoring, without notification, any information technology.

### **3.4.Vulnerability Management**

The Information Security Group (ISG) is responsible to monitor and report on vulnerabilities in Lowe's information technologies. The specific departments responsible for such information technologies must adhere to the requirements of the Lowe's *Vulnerability Management Policy* and follow these guidelines:

- Critical security patches must be applied in a timely manner from the date of release.

- A network-based virus scanning system must be employed to check files (containing executable content) as they are pulled or opened from any source.
- A platform-based virus scanning system must be employed on all workstations, server, and network devices that support the Lowe's virus scanning solution.
- Vendor updates for new malware signatures should be obtained daily and applied automatically.
- All alerts of malware must be reported to the ISG .

### **3.5. Technical Security Standards**

The ISG identifies, approves and monitors for the implementation and compliance of technical security standards to meet business, contractual, regulatory and legal requirements. Information technology configurations must comply with Lowe's security policies and standards.

### **4. Compliance**

Compliance with this Policy is mandatory and will be a matter for periodic review by Internal Audit and Information Security. Violations of this Policy may result in disciplinary action, up to and including termination of employees, termination of contracts and alike for external entities and compensatory damages for both.

### **5. Maintenance**

Change requests to this Policy must be submitted in writing to the Director of Information Security. The Director of Information Security is responsible for reviewing and approving change requests. (See the *Policy Change Request Form*).

### **6. Sponsor**

The Chief Information Officer is the Sponsor of this policy. The Director of Information Security is responsible for its maintenance and accuracy. Any questions regarding this policy should be directed to the Director of Information Security.

### **7. Custodian**

The Director of Information Security is the Custodian of this policy and is responsible for enforcing compliance. Any questions regarding the enforcement of this policy should be directed to the Director of Information Security.

### **8. Definitions**

<b>Term</b>	<b>Definition</b>
Information Assets	Any and all information or software used, processed and stored by Lowe's in the normal course of operation.
Access	The ability to view, process or otherwise use information assets.
Remote Users	Any individual using external services (Dial-up, Broadband, VPN, Internet, etc) to connect to Lowe's information systems.
Malware	Any executable file (program) whose purpose is the destruction or modification of files, self-propagation or other malicious activity.

This includes but is not limited to viruses, trojan programs, worms, etc.

**Sensitive information** Information that can be damaging to Lowe's or its customers' reputation or market standing if inappropriately handled or released. See the *Lowe's Code of Business Conduct and Ethics*.

**Unauthorized Disclosure** The intentional or unintentional revealing of information to people, both inside and outside of Lowe's who are not authorized to receive such information and/or who do not have a need to know such information.

## **9. Revision History**

Initial Release replaces the 1999 version of the Corporate Data Security Policy.

Reviewed and approved by the Information Security Management Committee September 2004.