Information Security Policy

Anti-Virus, Malware Policy

Anti-virus Software

Anti-virus software must be installed on development, domain and production hardware devices which hold SalesNexus or SalesNexus client information, passwords. The most recent version of the anti-virus software update must be maintained on each of these devices.

Security Against Malware

In order to prevent the transmission of malware onto SalesNexus computing systems:

1. Establish policies prohibiting the use of unauthorized software and to protect against risks associated with obtaining files and software from external networks.
2. Conduct regular reviews of the software and information content of systems supporting critical business processes.
3. Identify unapproved or unauthorized software or content and investigate and remove or quarantine.
4. Perform regular updates to malicious code detection and repair software used to scan computers and media. Malware tests must include:
5. Check any files on electronic or optical media, and files received over networks, for malicious code before they are deployed for use.
6. Checking electronic mail attachments and downloads for malicious code before distribution.
7. Checking web pages for malicious code.
8. Develop procedures and identify responsibilities to address protection against malicious code on information systems.
9. Provide training in their use, reporting and recovering from malware attacks.
10. Prepare appropriate business continuity plans to recover from malicious code attacks, including necessary information and software backup/recovery measures.
11. SalesNexus personnel must be educated about hoaxes and what to do when one is received.

Backup Policy

Information Backup

Information Security staff will ensure a scalable backup system that automatically copies data on a regular schedule is operational in order to prevent the loss of business- critical information.

1. Backups of data will be encrypted to prevent unauthorized use.
2. Data backups must be stored in a remote location, at sufficient distance to escape damage from a disaster impacting SalesNexus facilities.
3. The SalesNexus Backup Plan includes accurate and complete records of backup copies and documented restoration procedures.
4. Backup Plans and scheduled will be constructed to meet SalesNexus's business needs, the security requirements of the information involved, and the criticality of the information to SalesNexus's continued operations.
5. SalesNexus personnel must monitor the execution of backup processes and address failures of scheduled backups.

Information Privacy Policy

Definition of Private Information

- All personally identifiable data.
- Authorization credentials, oauth tokens.

Controls over Private Information

- Private Information is stored only on systems that comply with SalesNexus Information Security Policies.
- Private Information are accessed only by authorized personnel with a documented business need.
- Access to Private Information is monitored and logged automatically.
- Incident Management Policy

Incident Responsibilities

Management responsibilities and procedures will be established to ensure fast and effective response to information security incidents guided by these principals:

- Inform affected persons and entities proactively.
- Mitigate risks as rapidly as possible.
- Coordinate effectively with concerned government or public entities.
- Document incidents, investigate causes and modify policies accordingly.

Incident Severities

Security incidents are categorized into distinct levels based on the severity of the incident, information at risk, potential for damage, and/or threat to the corporation or brand. Response standards procedures, and methods will be implemented based on these incident severities:

- Severity 1 ("High") – An event that can cause significant damage, corruption, or loss (compromise) of SalesNexus Confidential or Private information. The event can result in potential damage to customers or the public and liability to the Company and to its public

image and may degrade customer confidence concerning SalesNexus products and services.

- Severity 2 ("Medium") – An event that may cause damage, corruption, or loss of replaceable information without compromise or may have a moderate impact on SalesNexus's operations or reputation.
- Severity 3 ("Low") – An event that causes inconvenience, aggravation, and/or minor costs associated with recovery, unintentional actions at the user or administrator level, or unintentional damage or minor loss of recoverable information. The event will have little, if any, material impact on SalesNexus's operations or reputation.

Severity Events

- SalesNexus Personnel managing the Company's computing infrastructure who suspect an information security event has occurred or find a weakness in a system or application must immediately contact their supervisor, Information Security (security@SalesNexus.com) or the Incident Response Team (IRT).
- SalesNexus Personnel should not communicate any information security incident details to anyone other than their supervisor, Information Security or the IRT.
- Unless previously approved by Legal and Information Security, SalesNexus Personnel must not report or discuss security incidents, events, problems, and/or violations with outside parties (e.g. news reporters, researchers, independent organizations compiling reports about incidents, professional societies, and/or law enforcement personnel).

Communications

- The IRT will coordinate and maintain communications with SalesNexus management as well as affected business units throughout an incident.
- The IRT will also consult with Legal, Information Security, Corporate Communications and other relevant parties regarding any external communication requirements, including communications with partners, customers, vendors and law enforcement.

Managing Security Incident

- Events reported to supervisors or Information Security will be forwarded to the IRT for review and validation in order to determine if the Incident Management process needs to be activated.
- The IRT will assess a reported security incident, determine the severity classification and implement the appropriate response.
- The IRT will manage the incident response to completion including the identification, collection, acquisition and preservation of information in a manner that will allow it to serve as evidence in a security investigation and/or prosecution after the incident is closed.
- The IRT will ensure security incident records, including root causes and corrective actions, are documented and reported to affected parties and management. The

Information Security Policy will be updated accordingly.

Exposure of Restricted Information

In compliance with laws regarding the response to suspected or confirmed exposures of personal information (e.g. PII or HIPAA) if there is a suspected or confirmed loss of restricted information, Legal counsel and Information Security must be contacted immediately regarding:

- The information potentially exposed;
- Number of affected individuals;
- How the information was exposed;
- Immediate action taken to protect the continued exposure of the information.

The Legal counsel and Information Security will monitor the situation and convene a Risk Analysis Group to determine the level of exposure and the response.

- The group will determine if notification is required, if contact with individuals or customers is appropriate, and analyze the remediation activities to ensure the information is no longer exposed and how to prevent it in the future.