The Honest Advantage

READY TO CHALLENGE THE STATUS QUO

GSA Security Policy and PCI Guidelines

The GreenStar Alliance | 2017

Table of Contents

GreenStar Alliance Security Policy

The GreenStar Alliance concept was founded on the basis of building trust, and to serve our customers with the best values and services possible in the heating and air-conditioning industry. GreenStar Alliance (GSA) management and employees in addition to GreenStar Alliance members and contractors have an inherent responsibility to protect the physical information and assets of the company, as well as confidential member data and intellectual capital owned by the company. These critical assets must be safeguarded to mitigate any potential impacts to GSA and GSA's members. Information Security at GSA is, therefore, a critical business function that should be incorporated into all aspects of GSA's business practices and operations.

To achieve this objective, policies, procedures, and standards, have been created to ensure secure business practices are in place at GSA. Information security is a foundational business practice that must be incorporated into planning, development, operations, administration, sales and marketing, as each of these business functions requires specific safeguards to be in place to mitigate the risk associated with normal business activities.

GSA is subject to numerous State and Federal Information Security and Privacy laws and regulations, which if not complied with, could potentially result in fines, audits, loss of member confidence, and direct financial impacts to the company. Compliance with all applicable regulations is the responsibility of every employee at GSA.

Information Security Policy Overview

Everyone at GSA is responsible for familiarizing themselves with and complying with all policies, guidelines and standards dealing with information security.

DEFINITION OF INFORMATION SECURITY

The U.S. National Information Systems Security Glossary defines Information systems security (INFOSEC) as:

> *The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.*

Information Security centers on the following three objectives for protecting information: Confidentiality, Integrity, and Availability. The foundational concepts in this document support these objectives.

WHY SECURITY?

GSA requires information security to protect information assets from security threats. It is critical to protect the system environment to maintain a competitive advantage in the marketplace, to ensure profitability, and to secure and maintain member and partner trust and confidence.

Security threats originate at a wide variety of sources, including computer-assisted fraud, industrial espionage, sabotage, vandalism and natural disasters. Computer viruses, unethical hacking and denial of service attacks are examples of threats encountered while operating over the Internet. These types of threats are becoming increasingly more common, more ambitious and more sophisticated.

PHILOSOPHY OF PROTECTION

The GSA philosophy of protection provides the intent and direction behind our protection policies, procedures, and control. Our protection philosophy is comprised of three tenets:

1. **Security is everyone's responsibility**. Maintaining an effective and efficient security posture for GSA require a proactive stance on security issues from everyone. Security is not "somebody else's problem;" as a member of GSA you have the responsibility to adhere to the security policies of the company and to take issue with those who are not doing the same.
2. **Security permeates the GSA organization**. Security is not just focused on physical and technical "border control." Rather, GSA seeks to ensure reasonable and appropriate levels of security awareness and protection throughout our organization and infrastructure. There is no place in our business where security is not a consideration.
3. **Security is a business enabler**. A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within the marketplace, and must be treated as a valued commodity.

   The tenets of our philosophy of protection are mutually supportive; ignoring any one tenet in favor of another undermines the overall security posture of our organization.

_____
INITIALS

CRITICAL SUCCESS FACTORS

The following factors are critical to the successful implementation of security within GSA:

- Comprehensive security policies, objectives and initiatives that clearly reflect GSA business objectives
- A security approach that is consistent with GSA's culture
- Highly visible support from the GSA executive management
- Solid understanding of security requirements and risk management practices
- Effective communication of security to all GSA managers, associates, partners, clients, vendors and developers
- Guidance on information security policy to all GSA managers, associates, partners, clients, vendors and developers
- Information security awareness and training
- Continual review and measurement of the effectiveness and efficiency of security controls and mechanisms
- Timely adjustments to the security posture by addressing deficiencies and by reflecting changes in the GSA business objectives as necessary
- Annual review of the information security policy to update policy as needed to reflect changes to business objectives or the risk environment.

Security Policy

INFORMATION SECURITY POLICY DOCUMENT

GSA Executive Management will provide direction for, approve, publish, and communicate the merits of an Information Security Policy document. This Information Security Policy Document shall outline managements' approach to Information Security as well as providing the organization with a strong indication of the management commitment to Information Security within GSA.

The purpose of this policy is to communicate the direction of the organization's Information Security Program by providing relevant, accessible and understandable definitions, statements and explanations.

The Information Security Policy Document shall serve as a reference document that will lead to additional more detailed information when necessary (for instance employee manuals etc.).

INITIALS

BUILDING ACCESS

Only authorized GSA members and employees are allowed in the working areas of any GSA complex. Guest areas are defined and are open to everyone. Any non GSA member or guest must be accompanied whenever there is a need for a guest to enter any working areas.

COMPUTER AND SOFTWARE ACCESS

Any GSA provided system, or any system accessing the GSA network must have user specific password access.

General

- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 10 passwords.
- User accounts with access to sensitive software, such as account, customer relationship management system, must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

Password Requirements

To prevent any unauthorized use of your User Account, you must not share your Password with any third party. The password creation requirements must be applied as follows:

A. Be a minimum length of eight (8) characters on all systems.
B. Not be a dictionary word or proper name.
C. Not be the same as the User ID.
D. Expire within a maximum of 180 calendar days.
E. Not be identical to the previous ten (10) passwords.
F. Not be transmitted in the clear or plaintext outside the secure location.
G. Not be displayed when entered.
H. Passwords are only reset for the authorized user.

Password Protection Standard

Do not use your User ID as your password. Do not share GSA passwords with anyone,

INITIALS

including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential GSA information.

It is your responsibility to safeguard your password. If any account or password is suspected to have been compromised, report the incident and immediately change all passwords.

REVIEW AND EVALUATION OF INFORMATION SECURITY POLICY

The CEO shall be the owner of this Information Security Policy Document. The owner of the document shall be responsible for maintaining and reviewing the policy based upon a defined review process. The policy shall be reviewed at least annually and updated in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new regulations or changes to the organization's infrastructure.

The reviews shall include an assessment of the policy's effectiveness based upon:

- The nature and number and impact of recorded security incidents;
- Cost and impact of controls on business efficiency; and
- Effects of changes to technology.

INITIALS

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data, and include specific requirements for software developers and manufacturers of applications and devices used in the transaction process. Compliance with the PCI security standards is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

All GreenStar employees and members shall adopt the PCI DSS standard to ensure the safe and appropriate management of sensitive credit card information. GreenStar Alliance (GSA) shall always perform credit card transactions through PCI DSS compliant software. No information shall be recorded outside of the allowed software used to protect cardholder data.

NETWORK SECURITY

GSA shall periodically contract a third-party vendor to examine network traffic and confirm all systems are protected from unauthorized access from untrusted networks. GSA shall use trusted connections such as business-to-business connections, via wireless networks, or via other sources. The selected vendor shall provide a documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall.

The GSA network security shall be tested by a third-party vendor at least every six months, or whenever a modification to the network related hardware is required that may affect the network security.

The selected vendor shall provide network diagrams describing how networks are configured, and identify the location of all network devices. This is especially crucial for network and cardholder data-flow diagrams. This data helps an organization to understand and keep track of the scope of their environment, by showing how cardholder data flows across networks and between individual systems and devices.

If a GSA employee is exposed to private internet protocol (IP) address information, the shall not disclose this information to unauthorized parties. Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker “learning” the IP addresses of the internal network, and using that information to access the network.

INITIALS

SYSTEM PASSWORDS AND SECURITY PARAMETERS

Vendor-supplied defaults for system passwords and other security parameters must be reset and documented in a manner that provides adequate integrity of the GSA network. The vendor shall provide adequate security guidelines to protect the GSA network from outside or inside malicious individuals.

The third-party vendor must have configuration standards for all system components. The vendor must assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

Refer to the GSA Security Policy for additional information.

PROCESSING CREDIT CARDS

Within GSA, the solution will remain simple by using PCI compliant software to interface with and enter all applicable cardholder information.

At no time shall the cardholder information be recorded other than inside of the PCI compliant software authorized by GSA.

GSA currently approved software that accepts cardholder data is Payzer and Converge. Individual user accounts with limited capabilities will be prepared for the respective GSA employee for accepting member or customer cardholder information.

Even though QuickBooks has the ability to accept cardholder data, it is designed to be entered by the cardholder through the links provided by QuickBooks when invoices are issued for payment.

GSA uses a merchant service called Stripe. This is an online e-commerce PCI compliant software that GSA employs to allow members and customers to enter their credit card information to remit payment for their online or member purchases. Stripe returns non-sensitive card information in the response to a charge request. This includes the card type, the last four digits of the card, and the expiration date. This information is not subject to PCI compliance, so you are able to store any of these properties in your database.

INITIALS