PARTNERCOMMUNITY®

INFORMATION PRIVACY AND SECURITY POLICIES

2012

PartnerCommunity, Inc.

PartnerCommunity Confidential and Proprietary

PURPOSE

PartnerCommunity (PCI) recognizes the importance of preserving confidentiality and privacy. Furthermore, protecting the integrity of information is essential.

- Information and information systems are critical and vitally important PCI's and/or its customers' assets. Information security refers to preserving the confidentiality, protecting the integrity, and ensuring the availability of information.
- To be effective, information security must be a team effort involving the participation and support of every PCI colleague who deals with information and/or information systems. This means that PCI takes appropriate steps to ensure that information and information systems are properly protected in accordance with internal polices and local, state, and federal laws and regulations.

POLICY STATEMENT

The PCI Privacy and Security Policy provides guidance to all employees, board members, providers, agents, consultants, contractors, and suppliers in carrying out their daily activities. Throughout this document, this group of affected individuals is collectively referred to as "colleagues" of PCI. The obligations under this policy apply to PCI's relationships with its customers, subcontractors, vendors, consultants, Business Associates, and one another.

Access to PCI information and the sharing and security of that information requires that each colleague accepts responsibility to protect the rights of PCI. Any user of PCI resources who, without authorization, distributes, accesses, uses, destroys, alters, dismantles, disfigures or disables PCI information resources creates a threat to the secure environment of PCI. These actions are subject to discipline.

PROCEDURE

1. In the course of business, it is necessary for PCI to record, store, process, transmit, and otherwise handle confidential and private information about individuals, employees and customers. PCI takes these activities seriously and seeks to provide fair, secure, and legal systems for the

appropriate handling of such information. It is the intent of PCI to provide the policies, procedures, and training necessary to protect the privacy of sensitive information.

2. PCI may receive information about its customers, their networks, systems and processes. PCI does not release or discuss such information with any others unless it is authorized by the owner of such information in writing, or required by law.

3. Confidential information about PCI's strategies and operations is a valuable asset. This information must not be shared with others outside of PCI unless the individual has a legitimate reason to know and agrees to maintain the confidentiality of information. Any information release is mandated to keep a record to describe the details (who, what, when, where, why and how).

4. It is critically important to maintain customer confidentiality, as well as to maintain confidentiality about PCI employees and business information. This policy pertains to all information, (verbal, paper, and electronic) related to the operation of PCI including, but not limited to:

    - Employee names, including pay rates and employment information.
    - Marketing and general business strategies.
    - Financial information.
    - Any information received from a customer that is covered by a non-disclosure agreement.

5. In addition to the above, any information that has been marked "confidential" by PCI is deemed to be covered under this policy. Unauthorized access, use, or release of confidential and sensitive information to non-authorized individuals is strictly prohibited and may result in immediate disciplinary action up to and including termination.

6. This policy applies to all PCI subsidiaries, divisions, departments, and organizational units.

ACCOUNTABILITY AND RESPONSIBILITY

Maintaining information, privacy, and security is the responsibility of all PCI colleagues. The responsibility includes assuring compliance with PCI's polices for confidentiality by non-PCI employees performing work at, or for PCI. Business Associates, vendors, consultants, and subcontractors working with PCI, must be informed of their obligations regarding PCI information, privacy, and security polices and agree to consequences appropriate to any breach of such polices. Contracts must include language specifying obligations regarding privacy and security and consequences of a breach when appropriate.

User Responsibility: A "user" is any person who accesses any corporate data in any form. Each user is responsible for:

1. Maintaining the confidentiality of information.

2. Complying with PCI policies, standards, and procedures including those in this document.

3. Taking any reasonable and logical measure that is necessary to preserve information confidentiality and privacy even if it is not specifically addressed in a policy.

4. Maintaining a secure work area.

5. Safeguard output (such as printed reports, screen prints, copies, ancillary storage devices (USB Drives, etc.)).

6. Reporting an observed or suspected breach of information security to management.

7. Maintaining a secure digital signature.

8. Using only unique system login(s) and not allowing anyone else to use unique system login(s).

Managers/Supervisors are responsible for:

1. Establishing, publishing, and enforcing departmental standards and procedures to:
    a. Prevent unauthorized collection, disclosure, modification or destruction of data.
    b. Develop and maintain data security awareness among subordinates.
    c. Assure that the PCI standards and policies on the length of retention and destruction of information are followed.

2. Reviewing job responsibilities of a new or transferred employee, consultant/ tractor, business associate, or other user, and determining what access to functions/databases is needed to perform their job function.

3. Ensuring requested access is consistent with approved standards.

4. Requesting access by the fewest users necessary to ensure completion of work.

5. IMMEDIATELY notifying Information Technology (IT) when a user's access is terminated.

6. Ensuring staff are updated on PCI's information security standards/polices.

7. Informing users under their supervision of changes in policies, standards, or procedures.

8. Overseeing their employees' use of systems, internet and company resources and initiating appropriate disciplinary action.

IT is responsible for:

1. Ensuring and maintaining a secured system and network environment.
2. Managing system and network access control.

ACCESS TO AND USE OF INFORMATION AND SYSTEMS

PCI is committed to taking all reasonable and appropriate measures to protect sensitive information against accidental or unauthorized modification, disclosure, or destruction, including the security of the equipment, software, and data. Access to information is only granted on a need to know basis based on role and responsibilities.

1. Computer software, hardware, communication equipment, and encryption capabilities are assets of PCI. All data processing resources (e.g. software, servers, data), owned, used, or maintained by PCI are properly secured in accordance with these standards.
2. Use of PCI computers is primarily for PCI business-related activity or professional development. The electronic environment is part of the workplace and carries with it the same expectation of mutual respect and confidentiality that applies to all other activities at PCI.
3. PCI may use human or automated means to monitor the use of systems handling PCI information. Tools for monitoring or observation of computer user activities may be used with or without prior notification. The findings may be disclosed to management or law enforcement during the course of investigation.

PERSONAL OBLIGATION TO REPORT

All employees or colleagues of PCI, have a responsibility for reporting activity by any employee, subcontractor, business associate or vendor that appears to violate applicable laws, rules, regulation, or information privacy and security policies. Failure to do so could serve as a basis for disciplinary action.

COMPLIANCE

Failure to comply with confidentiality and information security policies, standards, and procedures may result in disciplinary action which includes termination or suspension of network access. Compliance means conformity to information security policies and standards as well as the information security procedures developed to meet user needs.

1. Managers have the primary responsibility for enforcing and monitoring compliance. Additional support for overseeing compliance is provided by IT.

2. Observance of information security polices, standards, and procedures is a condition of employment.