CAMPUS PARTNERS

Information Security Program

Even before the introduction of the Gramm-Leach-Bliley Act in May 2003, Campus Partners was acutely aware of the responsibilities associated with maintaining control over, and access to, information within its information systems. Campus Partners' reputation is directly linked to the way in which it manages both information and information systems. For example, if private customer information were publicly disclosed, the organization's reputation would be harmed. For these and other important business reasons, executive management working in conjunction with the Board of Directors has initiated and continues to support an information security program.

One part of that program was the creation of a corporate Information Security Policy. The Campus Partners Information Security Policy defines the responsibilities of users as well as the steps they must take to help protect Campus Partners' information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

Guidance, direction, and authority for information security activities are centralized for all Campus Partners organizational units in the Information Technology department. The Information Technology department is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures. Investigation of system intrusions and other information security incidents is the responsibility of the Information Technology department.

Security of Electronic Data

Logical Security

Information Security, organized as a unit of the Information Technology department, has responsibility for enforcing existing corporate information security policies and standards as well as researching and recommending enhancements and solutions to corporate information security problems. Campus Partners' corporate policy is that access should be on a "need to know" basis. This policy is applied across all corporate information systems and is reflected in written standards followed by the Security Administrators. Information Security is responsible for maintaining security within established corporate standards.

Access to Systems

To maintain the integrity of System III data, the on-line user must use a Campus Partners assigned ID and an initial password that must match a valid ID/password. External user access is limited to only loans associated with their System III assigned number for their institution. Once the ID and password are validated, any request to view a loan or borrower record not accessible to this user will produce a "Record Not Found" message on the screen. No information will be displayed identifying or even confirming the existence of any loans except those available to this user.

Campus Partners requires that passwords created to access system information must be at least six characters in length and passwords must also be changed every 90 days, or at more frequent intervals. Whenever a worker suspects that a password has become known to another person, that password must immediately be changed.

Human Resources, in conjunction with the Information Technology department, is responsible for maintaining a current list of employees and their position within the company to ensure that system access is kept current. To assist in this process, Human Resources produces a monthly report that details employees who have either left the company or who have relocated to a different area within the company. The Information Technology department uses this listing to review system access to ensure that the appropriate level of access is maintained, or removed if necessary.

Physical Security

Data processing operations are provided by Infocrossing Southeast, Inc. ("Data Center") located in Norcross, Georgia. Campus Partners utilizes the Data Center for mainframe and wide-area network (WAN) operations and support under a Shared Processing Facilities Agreement. Local area network (LAN) operations and support are provided internally by Campus Partners personnel at the Winston-Salem Service Center.

The data center is secured by magnetic card key, and access is restricted to those associates, building management and vendors with authorization and a business justification to enter the rooms. All computer room visitors are required to sign a computer room visitor log and be escorted by an authorized employee.

Human Resources, in conjunction with the Facilities department, is responsible for maintaining a current list of employees and their position within the company to ensure that building access is kept current. To assist in this process, Human Resources produces a monthly report that details employees who have either left the company or who have relocated to a different area within the company. The Facilities department uses this listing to review building access to ensure that the appropriate level of access is maintained, or removed if necessary.

Environmental Controls

The Data Center has environmental controls in place including an automatic Halon fire suppression system, smoke alarms, water detection sensors under the floor, hand-held fire extinguishers, and raised flooring. Climate control instruments are used to regulate temperature and humidity. An Uninterruptible Power Supply (UPS) with on-site generation is in place for all systems and workstations located within the Data Center. The UPS is connected to a Power Distribution Unit (PDU). The UPS can operate the computer systems for about 30 minutes. A diesel generator will start after the UPS batteries have been engaged for three minutes. The diesel generator will also start if the Data Center experiences consecutive short power outages of one to two minutes.

A timer monitors the power supply and will not turn off the diesel generator until there is an uninterrupted, constant power supply of at least 30 minutes. The timer starts over every time there is a change in the power supply. Computer systems are attached to a PDU to ensure that the correct amount of power is being supplied to the appropriate systems.

Virus Scanning

Viruses can be spread by data files and by program files. To assure continued uninterrupted service for both computers and networks, all personal computer users must keep the current versions of approved virus screening software enabled on their workstations. This screening software must be used to scan all software and data files coming from either third parties or other Campus Partners groups. This scanning must take place before new data files are opened and before new software is executed. Workers must not bypass or turn-off the scanning processes which could detect the transmission of computer viruses.

Security of Physical Data

Building Access

The Campus Partners facility shares a building with other tenants. However, access to the Campus Partners facility is controlled at the main entrance by a Security Guard and a magnetic card key is required to access the operational areas. Visitors are required to sign a visitor's log and have a Campus Partners associate escort them to their destination. After business hours, card key readers must be used to gain access to the facility. The magnetic card key is unique to each cardholder. Cardholders may not allow others, even other Campus Partners associates, to use their card keys.

Printed Material

To ensure the proper destruction of printed material after use, Campus Partners has placed repositories throughout the work areas where employees can place sensitive information that needs to be discarded. Campus Partners has contracted with a licensed and bonded third-party vendor for the removal of this material.

Confidentiality

Our Human Resources department maintains an Employee Handbook that contains the Campus Partners employment policies related to employee conduct, hiring and firing practices, employee benefits, and security information. Deviations from the Code of Conduct detailed in the Employee Handbook are investigated and responded to by management. Consequences of Code of Conduct violations may include termination. Due to the nature of the information they will have access to, new employees are counseled about the confidential nature of the information and are required to sign a non-disclosure agreement as a condition of employment.

Unless it has specifically been designated as public, all Campus Partners internal information must be protected from disclosure to third parties. Third parties may be given access to Campus Partners internal information only when a demonstrable need-to-know exists, and when a Campus Partners non-disclosure agreement has been executed and authorized by the relevant Campus Partners information owner.

Security of Information Transmission

Firewalls

Firewalls are an essential component of Campus Partners' information systems security infrastructure. Firewalls are defined as security systems that control and restrict both Internet connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced. Connectivity, as the word is used here, defines which computer systems can exchange information. A service, as the word is used here, is sometimes called an application, and it refers to the way for information to flow through a firewall. Examples of services include FTP (file transfer protocol) and HTTP (web browsing). The Campus Partners' Information Security Policy defines the essential rules regarding the management and maintenance of firewalls and it applies to all firewalls owned, rented, leased, or otherwise controlled by Campus Partners workers.

Auditing

Because firewalls provide such an important barrier to unauthorized access to Campus Partners' networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures.

Logs

All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged. These logs are promptly removed from the recording systems and stored in a physically protected container for at least six months after the time they were recorded. These logs are reviewed periodically to ensure that the firewalls are operating in a secure manner.

DMZs

All Internet web servers must be protected by firewalls in a demilitarized zone (DMZ). Demilitarized zones are subnets, which are protected by a firewall from the Internet, but themselves have another firewall preventing users of the systems in the DMZ from gaining access to other network-connected Campus Partners computers outside the DMZ.

Internet Security

The Campus Partners Web site provides access to information to both borrowers and customers via the Internet. This information includes account information, Campus Partners publications and company information. Students and customers can also access information about the various loan programs available, download necessary forms and view specific account information through these sites.

Specific account information is only made available to borrowers and customers after they have established an account with Campus Partners and then access is restricted to only those accounts that are directly related to that borrower or customer. Borrower and customer transactions are secured through the use of Secure Socket Layer (SSL) 128-bit encryption software.

Business Continuity

Disaster Recovery Planning

The Campus Partners' Data Center has a documented Disaster Recovery Plan (DRP) that outlines detailed procedures to be performed for the restoration of processing in the event of a facility disaster. A copy of the DRP is kept in an off site vault with run schedules, policies and procedures, services manual and contract, tape pull lists and tape boxes, tape library listings updated daily, extra tapes and office supplies, standard forms, manuals, phone lists, etc.

The DRP lists who has the authority to declare a disaster, the recovery team leaders and team members, and vendors and customers that need to be notified in the event of a disaster. It also includes procedures for obtaining emergency funding, roles and responsibilities of the various functions, DRP testing, network maps, and the role of Infocrossing Southeast in the event of a disaster. IBM is contracted to provide a warm site which contains terminals that allow operators to remotely operate the hot site. The hot site contains CPUs, peripherals, and other principal equipment. In addition, there is a Primary Customer Control Center for Computer Operations, a Network Control Center, both located in Wood Dale, IL. These sites also provide office space, printers, telephones, faxes, and support services.

The Data Center tests its DRP annually to ensure it is current. Campus Partners takes part in the recovery test to ensure that the Winston-Salem Service Center can be operational in the event of a disaster.

Business Continuity Planning

Campus Partners has developed a Business Continuity Plan (BCP) for the Winston-Salem Service Center. This plan is designed to represent the processes Campus Partners will employ to ensure that the assets of the company are protected and the business of the company may be re-established in the event of a disaster. Campus Partners has established guidelines for emergency situations that detail processes to follow in cases of fire, bomb threats, serious injuries, severe weather, and general security.

External Reviews

Campus Partners currently has a SAS-70 audit performed annually by an independent auditing firm. This audit, while not a requirement of all programs serviced by Campus Partners, presents an opportunity for Campus Partners to have an independent, third-party organization review its processes and procedures related to the handling and processing of data on its servicing systems. The SAS-70 review focuses not only on the processing of data, but also the logical and physical security measures around that data. In addition, periodic reviews are performed by the Audit and Compliance department within Campus Partners to determine the levels of compliance with internal processes and procedures related to the processing of data and information.

Information Security Coordinator

Campus Partners has designated an individual to function as Security Coordinator over data and systems. This individual is:

John L. Elliott
Director of Information Technology
(336) 607-2365