

Webcom Data Center Information Security Policy

Introduction

Webcom takes security extremely seriously, and we make every feasible effort to protect our customers, as well as our selves. Webcom views trust as a privilege and we work diligently to maintain the highest level of security practical. The purpose of this policy is to establish direction, procedures, and requirements to ensure the appropriate protection of Webcom information, and for client information on devices located at Webcom's Data Center.

This policy has two purposes:

- Emphasize for all Webcom employees and contractors the importance of security in the various network environments and their role in maintaining that security.
- Assign specific responsibilities for the provision of data and information security, and for the security of the various systems.

This policy applies to all Webcom Solutions employees, contractors, and consultants at all Webcom locations. It applies equally to network servers, peripheral equipment, workstations, and personal computers within Webcom . The network resources covered by this policy include data, information, software, hardware, telecommunications, and all related facilities. It is the policy of Webcom to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information.

Physical Security

Physical security is concerned with preventing unauthorized access to data by preventing access to the hardware on which the data resides. At Webcom's Data Center, access is gained by passing through a two tier security access.

The first tier is access to the building. Access is only available between 8am and 5pm Monday through Friday. Unless you are authorized access is challenged beyond the front desk. At all other times the building is locked and access is only possible by using a valid security key. The security system is computer based and logs various information such as the identity of the person entering, date, time and the point of entry.

The second tier of security is access to the data center. The data center is a secure facility and access is only possible by a valid security key or FOB. Each employee, contractor or visitor is issued a FOB for access. For contractors or visitors access is limited to a set time period and therefore expires. Every entry into the data center is logged by the computer. All contractors or visitors without a FOB require an escort. No employee, contractor or visitor should give their FOB to anyone else.

The data center incorporates monitoring of the environment to insure that data is not subject to loss by extremes of temperature and humidity. In the event that temperature or humidity are out of normal operating parameters, the building's HVAC maintenance support team is automatically paged.

The data center also has a waterless fire suppression system, and if a fire occurs the FM200 fire suppression system will release and the fire department is notified by the security system. The City of Wauwatosa Fire Department maintains an engine company less than 1000 yards away from our facility.

Media and Documentation

All sensitive customer media and documentation is stored in the secured data center. All backup data is stored in the secured data center with the exception of offsite backup storage which is also in a trusted secure location.

Data Security

This policy enumerates specific responsibilities necessary to carry out this policy. Two classes of users are defined for this purpose: users and network managers. The specific responsibilities of each group is listed below. Users are expected to have a basic knowledge of computers and understand and adhere to Webcom security policies and procedures. User responsibilities include:

1. Selecting and maintaining good passwords.
2. Maintaining the password integrity by not disclosing them to others.
3. Employing all available security mechanisms for protecting the integrity and confidentiality of their information when required.
4. Installing a password protected screen saver to secure access to their PC when they are away from the PC.
5. Notifying the Manger of Information Technology if a security violation is observed or detected.
6. Users must not test or attempt to compromise computer and communication security measures unless they have been approved in advance by the Manger of Information Technology.

www.webcomforce.com

CONFIDENTIAL

Network managers are the individuals responsible for enforcing Webcom policies as they relate to the technical controls in hardware and software, archiving critical programs and data, and to control access to network physical facilities. The specific responsibilities for network managers include:

1. Securing the network environment within the site and connections to outside networks.
2. Responding to emergency events in a timely and effective manner. If the nature of the situation warrants, the Disaster Recovery Plan will govern the specific response.
3. Respond to security alerts.
4. Develop appropriate procedures for the prevention, detection, and removal of malicious software.
5. Conduct periodic reviews to ensure that proper security procedures are followed.

Network Security

Webcom 's Data Center utilizes several tools, both proactive and reactive, in order to maintain security and to respond to intrusions or other attempts to breach security.

Proactively, we use a Microsoft HFNETCHK and Microsoft Baseline Security Analyzer to evaluate security needs to our servers and workstations. We incorporate HFNETCHK into an automated batch process that runs weekly and reports the results to our help desk who in turn update the systems. The results are written to a text file for [reference](#) on our Intranet.

Proactively and reactively, we use a real time intrusion detection system (IDS) to monitor for intrusions or the precursors to an attack, e.g., port scans. Our IDS monitors all network segments at the Webcom Data Center, and is a managed service provided by [SecurePipe](#). Events are responded to in real time 24 by 7, with the response escalation determined by the nature of the attempt. When an attack occurs the Webcom Data Center help desk is notified and the on call network engineer is notified to respond. The procedure for notification is as follows: When SecurePipe determines that there is an event they will notify the Webcom Data Center Support Team.

Virus Protection

Webcom's Data Center has virus protection on all systems. The virus scanning is enforced from a central console for any user authenticating to the Webcom network. Multiple virus scans are also performed on email, including attachment filtering.

Access Control Guidelines

Log-In/Log-Out Process: All authorized persons must be positively identified before being granted access to system resources. Positive identification requires the use of a User ID and a password. All computers, routers, and firewalls connected to the data center network must have password access controls implemented. No device, or service account is permitted that does not have a password. In the event that system or network security is compromised or if there is reasonable belief that it may have been compromised the following actions will be taken:

1. Change all administrator and service account passwords.
2. Log the incident in Ticket Tracking System

User passwords are subject to strict standards to prevent intruders from pretending to be a legitimate user and authenticating to the system. The following user password measures have been implemented as part of this policy:

1. Only one user may use an account. Passwords are not to be revealed or shared with anyone else.
2. All vendor supplied and default passwords are changed immediately.
3. Passwords are changed every 90 days and will be enforced as a Windows user policy.
4. Passwords are a minimum of 6 characters.
5. Password uniqueness is enforced as an element of the Windows user policy.
 1. Not contain all or part of the user's account name
 2. Be at least six characters in length
 3. Contain characters from three of the following four categories:
 1. English uppercase characters (A through Z)
 2. English lowercase characters (a through z)
 3. Base 10 digits (0 through 9)
 4. Non-alphabetic characters (for example, !, \$, #, %)
 4. Complexity requirements are enforced when passwords are changed or created.
6. Passwords should be difficult to guess and should incorporate both letters and numerals.

www.webcomforce.com

CONFIDENTIAL

7. Passwords must not be a word found in the dictionary, a proper name, place, or slang.
8. Passwords used on systems are not be used on any outside computers.
9. Passwords should not be written down and left in places where unauthorized persons might read them.
10. All passwords must be immediately changed if they are suspected of having been disclosed, or known to have been disclosed to anyone.

Data Network Access Security: In addition to strong passwords it is necessary to implement packet filtering (firewalls) and router access control lists to prevent unauthorized access to network devices.

Router access lists have been established on the boundary router to restrict access into the network and to prevent IP address spoofing from the non routable private networks. Additionally, hosts believed to have attempted intrusions are blocked. Third, packet filtering occurs to detect virus or other malware signatures and prevent their transmission into the network.

Once the boundary router passes a IP packet to the Webcom Data Center network, it passes through a firewall. Our data center uses redundant Cisco PIX 515 firewalls to perform state full packet filtering. Depending on the destination of the packet, the firewall will either pass the packet to the host, or will block the packet based on protocol.

Currently, the firewall rules are as follows:

1. Web traffic is permitted in to the network on ports 80 and 443.
2. FTP traffic is permitted into the network.
3. SMTP traffic is permitted into the network.
4. All other protocols are denied or only allowed to a specific host as required to meet data center or client requirements for VPN and SQL.

Audit

In addition to responding to daily security alerts, Webcom periodically performs internal security audits. This includes the review of this security policy in addition to a vulnerability scan. Webcom reviews and corrects critical alerts immediately as it is practical to do so.

Our data center has undergone several external, third-party audits commission by our customers. In each case, reviews and corrects critical alerts immediately as it is practical to do so.