Tidewater Council Internet & Remote Access Security Policy March 22, 2016

Overview

Information is one of Tidewater Council’s most valuable assets, and each employee is responsible for helping to protect the privacy and integrity of member information and sensitive business information. The following requirements are designed to minimize the potential exposure to Boy Scouts of America from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may result from unauthorized access and use of Tidewater Council’s data or systems.

Policy

All employees and other authorized users, including external business partners, are expected to secure Boy Scouts of America member and corporate information and to protect the integrity, confidentiality, and availability of this information. Information security guidelines, procedures, and standards must be followed with regard to the use of Boy Scouts of America owned and leased equipment, computer systems, and networks. BSA provides computer and network resources for authorized use only. It is the policy of the Tidewater Council to adhere to the following technological internal control requirements.

Control Requirements

Internet security: All Internet connectivity to the local area network (LAN) must be accessed through the nationally provided and managed firewall device.

a. **Websites**: All websites must be hosted with an off-site Internet service provider and shall not have a direct connection or reference to the LAN.

b. **Email**: All Internet email services, other than BSAMail, must be hosted with an off-site Internet service provider (ISP) and relayed to the LAN from the ISP through the nationally provided firewall using a secure connection.

c. **Virtual Private Network (VPN):** All remote connections to the LAN shall utilize the nationally provided firewalls' VP service which will authenticate the request as a valid ScoutNET defined resource. Access to this service shall be authorized by the Scout executive or authorized designee.

1. Remote access of council resources:

a. **Dial in Modem Services**: All direct dial in remote access connections to any device attached to the LAN, including PCs, shall be prohibited; with the exception of modems required for monitoring and maintaining nationally provided systems (i.e., ScoutNET router and supply systems)

b. **Dial out Modem Services**: Modems used to dial out to other business partners, such as banks, shall be disabled when not in use (i.e., powered off). These devices shall not be left unattended while active.

c. **Wireless Network Equipment**: The purchasing, configuration and installation of any wireless network equipment shall be coordinated thru Network Services at the national office. All wireless access points shall connect to the network "outside" of the council firewall, users are required to use the VPN service to access the LAN through the wireless hub and all wireless traffic shall be encrypted using the wireless hubs' strongest recommended encryption algorithm.