

Rules of Behavior

TechSolutions.gov

(TechSolutions)

January 2009

TechSolutions is an outsourced information technology service established by the DHS Science & Technology Directorate. DHS 4300A Sensitive Systems Policy requires system specific Rules of Behavior to be defined for all IT systems. This Rules of Behavior documents the expected behavior of Booz Allen Hamilton and Xservices Privileged Users when accessing and using the system. Rules of behavior that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of sensitive information. Rules of behavior inform users of their responsibilities and let them know they shall be held accountable for their actions while they are accessing DHS owned systems. DHS 4300A Sensitive Systems Policy requires Components to define Rules of Behavior for all IT systems and ensure that users are trained regarding these rules and are aware of the disciplinary actions that may result from non-compliance. Additionally, users are required to agree to and sign these Rules of Behavior prior to being granted access to any DHS IT systems or data.

The following Rules of Behavior are to be followed by all Privileged Users of TechSolutions and are intended to clearly delineate responsibilities of, and expectations for, all individuals with privileged access to the system. A TechSolutions Privileged User is defined as any individual having the following system access:

Application Administrators are members of the TechSolutions SharePoint Administrators group and are tasked with administering the application and its content via the SharePoint Server console. Specifically, Application Administrators are responsible for creating, maintaining, and monitoring administrative accounts at the application level and updating application-level configuration and system and security patches. In addition, Application Administrators respond to application-level security incidents and investigations and work with DHS S&T security management toward incident containment, eradication, and recovery.

TechSolutions Configuration Managers are solely responsible for any/all modifications to the production application (to include code and content). TechSolutions Configuration Managers (or temporary delegates) will be the ONLY users approved to modify TechSolutions code or content in its production environment.

Security Administrators are users specifically privileged to oversee and/or directly implement and maintain security specific controls and configurations at the Operating System (system), database, and application levels. Additionally, Security Administrators are the only users privileged to modify TechSolutions audit logs (including those provided by Microsoft Windows 2003, SQL Server 2005, SharePoint, and TechSolutions custom code). No other users will be privileged to modify or delete

any audit logs associated with the TechSolutions system in order to promote separation of duties and prevent any other users from modifying or deleting records of their activities.

System Administrators are XServices staff responsible for the administration and maintenance of the TechSolutions servers (hardware and platform software such as Windows Server 2003 and SQL Server 2005) and supporting infrastructure. System Administrators are the only users privileged to create, modify, or delete domain, server, and database accounts (Windows 2003 and SQL Server 2005). System Administrators are not privileged to create, modify, or delete Application Administrator accounts via the SharePoint administration console (this is the purview of Application Administrators only). Additionally, System Administrators are responsible for system and application backups, system recovery, Windows 2003 (to include Internet Information Services 6.0), and SQL Server 2005 upgrades and patches, virus detection and eradication, network maintenance (firewalls, routers, switches, etc.), and setting up SSL VPN accounts to provide users with a secure SSL encrypted connection to remotely manage their environment.

The TechSolutions Information System Security Officer (ISSO) will ensure that all Privileged Users read and acknowledge these rules before being granted access to the system and again on at least an annual basis. The ISSO will maintain a current list of all users and will ensure that signed Rules of Behavior are on file for each user.

Any violation of the Rules of Behavior shall be considered a security incident, and will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation. In some cases, the individual may also be subject to criminal prosecution.

Account Creation:

- Users shall be provided access to TechSolutions based on their roles and responsibilities and granted rights according to “need to know” and “least privilege”.
- Users shall understand that their use of the TechSolutions system may be monitored and they acknowledge consent to this by signing this document.
- Users shall work within the confines of the access granted and shall not attempt to access systems or applications to which access has not been authorized.
- Users shall not circumvent or attempt to circumvent any security countermeasures or safeguards.
- All users shall have individual accounts. Shared accounts will not be permitted.
- All accounts shall have unique usernames and passwords.
- All accounts shall be removed when a user no longer requires access or after 90 days of inactivity.
- All passwords shall meet the following password requirements:

- Passwords are at least 8 characters long and have a combination of letters (upper- and lower-case), numbers, and special characters.. Null passwords are not allowed.
- Passwords must be changed every 90 days.

Password Protection:

- Users shall protect their password from disclosure.
- Users shall be responsible for any computer activity associated with their username and password.
- Users shall not reveal their password to others.
- User shall not write down or post their password in their work area.
- Users shall notify the ISSO immediately if it is believed their password has been compromised.
- Users shall have password protected screensavers that active after five minutes of inactivity.

System Access:

- Users shall not enter into any computer system without authorization. Any unauthorized entry into a protected computer file is a serious security violation and may result in civil or criminal prosecution depending on the extent of the violation.
- Users shall not attempt to circumvent or defeat security or auditing systems without prior authorization from the ISSO, other than as part of an authorized system testing or security research.
- Users shall not permit an unauthorized individual (including spouse, relative or friend) access to any sensitive computer network.
- Users shall acknowledge that modifying or altering the operating system or configuration of any system without first obtaining permission from the ISSO is prohibited.
- Users shall understand their responsibility to protect all output generated under their account to include printed output, magnetic tapes, and floppy disks.
- Users shall understand that there is no expectation of privacy and that their activity is subject to auditing while on TechSolutions.
- Users shall agree to notify the ISSO when access to TechSolutions is no longer needed.
- Users shall complete the required security awareness training courses and any system specific training prior to receiving access to TechSolutions.
- Users shall understand that a copy of this agreement will be kept on file with the ISSO as part of his/her security agreement.

Website Content:

- Information or content posted to the website shall be applicable to TechSolutions.
- No classified information shall be posted on TechSolutions under any circumstance.
- Users shall not store or process sensitive information on any system not explicitly approved for processing of that type of information.
- Any personal information submitted by Public Users to TechSolutions, such as email addresses, telephone numbers, street addresses, shall be for official use only and shall remain confidential.
- Users shall not place any malicious code, inappropriate language, pornographic or discriminatory material, or sensitive data on this website.
- All changes and modifications to content shall be approved following the TechSolutions change control process prior to it being displayed on TechSolutions (refer to TechSolutions Configuration Management Plan).
- Approved content changes shall be reviewed by the ISSO.

Protection of Media

- Removable media (backup tapes) are to be handled only by authorized individuals and stored in access controlled facilities, locked rooms, and locked cabinets marked 'FOUO'.
- Hard copy produced during code development is to be stored in locked cabinets or shredded in the shredders provided on all floors of the Booz Allen facility.

Protection of software copyright licenses:

- All copyright license agreements associated with the software associated with the website shall be made available to the ISSO.
- No new software shall be loaded to the TechSolutions website without prior coordination and approval by the ISSO.
- No hardware changes shall be made to the TechSolutions environment without prior coordination and approval by the ISSO.

Security Reporting Requirements:

- Users shall promptly report any observed IT security incidents or suspicions of security violations to the ISSO.
- System Administrators shall be required to receive DHS approval prior to any required changes for TechSolutions components (hardware/software). A documented Change Request of the required change must be submitted to the ISSO and DHS approval must be received prior to any changes being made to the system security environment.

Acknowledgement. I acknowledge that I have received as well as understand my responsibilities and will comply with the Rules of Behavior for the TechSolutions system. As a Privileged User of TechSolutions, I acknowledge my responsibility to conform to the above requirements set forth by the TechSolutions Program on behalf of the Department of Homeland Security. I understand that my failure to sign this Rules of Behavior will result in the denial of access to TechSolutions and its system components.

Privileged User (Print Name): _____ Date: _____

Privileged User Title: _____ Date: _____

Privileged User Signature: _____ Date: _____

ISSO/Security Officer: _____ Date: _____