ATTACHMENT 16

WESTAT INFORMATION TECHNOLOGY AND SYSTEMS (IT) SECURITY POLICY AND BEST PRACTICES

Westat Information Technology and Systems (IT) Security Policy and Best Practices

Westat is committed to observing high standards of information technology and systems (IT) security in order to protect the confidentiality, integrity, and availability of project and corporate information systems and the data they contain. Given the complexity and pervasiveness of today's information technologies and systems and the many different facets of systems and data security, the purpose of this IT Security Policy and Best Practices document is to provide "a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization," as recommended in the ISO/IEC International Standard 17799:2000E "Code of Practice for Information Security Management."

The objective of all Westat IT security policies and practices is to protect systems and data from a wide range of risks, to comply with the various legislative and contractual requirements of our clients, and to educate our staff regarding their responsibilities to comply with these policies. This document is reviewed at least annually by the Corporate Officer for Systems Security (COSS) and other senior management, and is amended or supplemented in response to new industry developments in IT security and relevant security risks or events that may arise from time to time.

Westat's IT security policies and best practices are organized into several broad areas: facility and computer security, data security, network and data communications security, personnel security, disaster recovery, and user assistance and incident reporting. These policies recognize that Westat's business is to provide contract services performing a wide variety of activities for a large number of clients using many different systems and computer programs, many of which are custom-developed for particular projects. Individual projects or clients may require variations that enhance the baseline intent of these security policies and practices. In developing specific project IT security plans, project staff are to make reference to the policies and practices described below and may also refer to additional resources such as the National Institute of Standards and Technology (NIST) Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems"; the International Standards Organization (ISO) standard 17799:2000, "Information Technology – Code of Practice for Information Security Management;" and relevant client- or agency-specific standards and guidelines.

Westat's COSS, reporting to the Director of the Computer Systems and Applications Staff, oversees the development and application of company information technology and systems security policies and best practices, and monitors conformance to these policies and best practices throughout the organization. The COSS also maintains an online archive of systems security information, including relevant detailed memoranda, instructions, and external reference documents, to guide and assist staff in planning and implementing systems security.

1. Facility and Computer Security

Access to Westat facilities is controlled at all times through the use of magnetic key cards assigned to individual staff, certain contracted consultants, and, in a few cases, selected vendor staff with established long-term business relationships. In addition, all staff are issued photo identification cards which must be visibly displayed at all times. Every use of the magnetic key card to enter a particular building or area is recorded in an electronic log for security and tracking purposes. Visitors are required to sign in with a receptionist and receive a day pass.

Access to the computer centers is also controlled by the key card entry system, with limited access privileges for designated operations and project support staff only. These specially designed centers house the computer systems, equipment for data communications, network services and operations, and high-speed printers. Special secured areas are established for sensitive data processing functions such as storing and printing of confidential data based on project requirements.

Westat buildings are protected against fires by automatic smoke detection and overhead sprinkler systems in accordance with local building and fire codes. These systems are centrally monitored by a fire panel that automatically dispatches the local fire department to arrive within minutes at our location in the event of an alarm condition. Computer facilities are equipped with redundant air conditioning systems to control temperature and humidity and are monitored 24 hours a day, with alarms providing notification of any abnormal conditions. Computer facilities are also protected against electrical power surges and short-term outages by battery-based uninterruptible power systems (UPS) and against fire by a chemical fire suppression system specifically designed to reduce the risk of damage to computer equipment and storage media that would result from a water-based system. Diesel-powered backup generators support the continuous operation of the data centers in case of long-term utility power failures.

Access to secure computer systems is password protected. All server and network data storage areas are protected by access privileges, which are assigned by the appropriate system administrator. Login passwords are encrypted and stored only in their encrypted form in protected files on each system.

A non-displaying or non-printing feature prevents the password from appearing on the computer screen during the login process. The system automatically limits the number of unsuccessful attempts to log in, after which the account is disabled and must be reset by the system administrator. To ensure the confidentiality of passwords, users are required to change their network passwords every 90 days. Passwords must be of a minimum length, must meet certain character and numeric usage rules, and cannot be reused. Accounts that have not been used for 90 days are automatically disabled and deleted within 1 week upon notifying relevant managers.

Only computer operations managers and designated server administrators have the privilege to bypass user mode restrictions in accessing a system to perform general system maintenance activities. All other users are restricted to user mode, which limits access to authorized servers and network storage areas and a subset of operating system commands and functions.

Purchase, installation, maintenance, and disposal of all server and PC hardware are performed by Westat's PC Technical Services group, and repairs and component replacements are completed on site. Requests to purchase and install enterprise software (e.g., software that is relatively expensive, requires a signed license agreement, or will be used by several or possibly all staff) may only be authorized by corporate officers. Special use software is relatively inexpensive software licensed by Westat that can be locally installed, supported, and used by individual staff, a project, or a study area, with manager approvals. The approval process includes consideration of the security features of the software. Special use software must be licensed to Westat through Westat's Purchasing group and may only be installed on Westat equipment in accordance with Westat's software policies (see "Westat's PC Software Policies" memo for further information).

2. Data Security

Westat assumes responsibility for the security of data in three forms of media: electronic storage (e.g., tape, disk, CD); hard-copy storage; and electronic transfer (e.g., via telephone or Internet transmission). Efforts are directed primarily at preventing any form of data security violations, whether they result from malfunction of the computer system, environmental hazards to the facility, or accidental or intentional misuse or misappropriation of data or systems. Monitoring of these security efforts is achieved through carefully planned management practices, control procedures, and facility and equipment standards, which are discussed below.

Each network storage directory is assigned an owner when it is created. Access to network-based data files is controlled through the use of directory and file access rights based upon user account ID and

the associated user group definition. Access rights are granted to specifically authorized users by the directory owner or the system administrator.

Database management systems have additional extensive security features. Regardless of the implementation platform, we require personal accounts for all users so database activity can be traced to individuals who have logged on using the password specific to that account. Accounts are assigned privileges based on the functions of the user within the application. Resource privileges and data definition privileges are restricted to accounts for programming staff. Database administration accounts are assigned only to trained, authorized senior staff. Passwords on critical accounts are changed periodically. Generally, system auditing is implemented for commands related to data definition, security administration, and logon failures.

Confidential or sensitive information is protected during transmission to and from Westat computer systems by the use of various data encryption technologies, such as Secure Socket Layer (SSL) and digital certificates and signatures that encrypt data, validate data integrity, and authenticate the parties in a transaction. Westat's internal network is a switched network that directs data flow over a limited set of specific paths, making it much harder to view or intercept data that is in transmission within the network.

Westat also supports a digital signature system that is a Public Key Infrastructure (PKI) server that provides digital and electronic signature support as well an encryption and decryption. This system uses a FIPS 140-1-certified PKI system from Entrust Technologies (Entrust/PKI) and supports FDA 21 CFR Part 11 security requirements. Projects or systems requiring these capabilities are provided with these technologies, systems, and expert staff consultation as part of Westat's corporate systems infrastructure.

Because electronic information is a valuable asset, several steps are taken to prevent the loss or corruption of data in case of equipment or facility failure. First, users are instructed to store all data files on network server directories rather than local PC hard disk drives. Second, Westat's Computer Operations staff backup all server-based storage to tape on a daily basis. A full disk backup is performed once a week and the tapes are retained for 4 weeks. An additional backup is created every fourth week and retained for 1 year. A daily incremental backup is performed the remaining 6 days of the week that copies any files changed that day to tape. The incremental backups are also retained for 4 weeks. Third, as an additional precaution, all backup tapes are removed daily from Westat's premises and transported in secure containers to an off-site storage facility that specializes in transporting and storing electronic

media. Tape identifiers for all backup tapes are maintained in a central tape management system for easy reference and retrieval.

Westat personnel are instructed in the importance of protecting data confidentiality, and all staff are required to read and sign Westat's **"**Employee or Contractor's Assurance of Confidentiality of Survey Data.**"** Data collected in hard-copy form are generally kept in locked cabinets or areas when not in use, depending on project requirements. Signs restricting access are posted at the entrances to secured data processing areas. Likewise, system-generated output containing confidential data is stored in locked areas until no longer needed and is disposed of in accordance with project requirements.

While labeled materials alert project staff to the sensitive nature of the contents, they may result in unwanted curiosity that may lead to an otherwise avoidable breach of security. Westat uses secure media storage, monitoring, and management practices to offset the need for obvious special labeling. Receipt control systems are designed to track the location of paper documents and, thus, detect any missing materials.

Project documents are kept for the duration of the agreed-upon retention period. Long-term offsite storage of materials is handled by a reputable and bonded firm. When the retention period has expired, the owner of the documentation is contacted to determine if the contents should continue to be retained or if the boxes of documentation should be destroyed. If the owner wants to continue to retain the information, the retention date on the box is modified. If the materials are no longer needed, they are securely destroyed (shredded or burned or magnetically erased).

Project staff are required to comply with Westat's "Electronic Data Storage, Transport and Security Acceptable Use Policies and Guidelines." They are also instructed to use Westat's Archive Tape System (WATS) to archive online data to tape. The WATS system includes a manager notification and corporate archivist review procedure for all archive and retrieval requests. In addition, WATS maintains a historical log of all project archive activities for future reference if necessary. Archive tapes are sent off site to a reputable and bonded external secure data storage firm for safekeeping.

PCs, workstations, and server storage devices that are being destroyed or discarded have low-level reformatting or other industry-approved destructive methods for destroying any data on the devices. Directories and their files that are no longer needed are removed, based on project requirements. These operations may be performed by Westat or an approved, certified equipment recycling company.

Project media (tapes, CDs, zip drives, etc.) that contain data, but are no longer serviceable, are destroyed by degaussing, low-level formatting, or other industry-approved destructive methods. Project media that can be reused have low-level reformatting or other industry-approved destructive methods for destroying any data on the media before being released back into use.

For paper records that need to be destroyed, Westat has several methods of destruction available for project staff. The following are located throughout Westat office spaces:

- Stand-alone paper shredders
- Non-secure paper recycling containers for NON-SENSITIVE documents
- Secure paper recycling containers for SENSITIVE documents

3. Network and Data Communications Security

Westat provides communications to host systems and servers through local area network-connected PCs, through some authorized high-speed encrypted virtual private network (VPN) connections to our firewalls, and, for some systems, through authorized low-speed dial-up connections. Access to host and server resources through these various connections is closely monitored, and system logs are regularly examined using automated tools to identify suspicious behavior.

Westat's network consists of a system of redundant firewalls and redundant Internet connections to support web sites, email, list servers, and FTP access for projects and corporate functions requiring these services. Westat's systems are kept separate from the general Internet by the programmable firewall that filters packets based on source address, destination address, and requested service. Several network zones with varying levels of access restrictions have been established on the firewall. With this configuration, resources that require fairly restricted access controls, such as database servers, can be kept separate from resources that need to be more generally accessible, such as web servers.

Intrusion detection software running on our firewalls detects and blocks outside users who are identified as attempting to gain unauthorized access to our network. Intrusion detection signature patterns are automatically updated regularly by the firewall application vendor to keep pace with the latest techniques used to break into networks.

The following are some key Westat network security zones that are used to protect internal systems from public Internet security risks:

- A Web Zone that allows access from the Internet for HTTP or FTP protocol access only. No other protocols are allowed. Production web servers providing project and corporate web sites to the public Internet are installed in this zone and include additional security features at the server and application level to prevent unauthorized access.

- A Data Zone that allows access only to designated applications running on Westat Web Zone servers. These servers act as proxy agents for authorized web users or designated internal Westat users. Direct access to this zone is not allowed from external Internet users or systems. In addition, database servers in the Data Zone are further protected through the use of server operating system, Oracle, or SQL Server access control features.

- The Wesnet Zone consists of Westat's internal network, servers, and workstations and is not accessible from the public Internet.

Applications that require stronger authentication protections may utilize individually assigned user certificates, smart cards, or other user authentication technologies. Data encryption during transmission to and from web servers is supported through the use of Secure Socket Layer (SSL) technology. This proven security protocol is widely used to support e-commerce transactions, server account authentication, data encryption, and digital signatures. Westat uses SSL for all restricted-access web sites involving confidential data.

Westat contracts with a qualified network security firm to conduct network security penetration testing to identify possible vulnerabilities to Westat systems from the public Internet. This test is performed at least twice annually. Separate penetration tests of resources located in the Wesnet and Data Zones are also performed twice each year. All results of the tests are received by the Corporate Officer for Systems Security (COSS) and formal reports of any identified server or system vulnerabilities are made to the appropriate systems technical administrators and managers who are required to respond with information on any corrective actions taken. Once all results and responses have been reviewed and any necessary corrective actions have been taken, the COSS makes a formal report by memo to the Director of the Computer Systems and Applications Staff that the security test cycle is completed and closed.

As a further measure, Westat periodically monitors traffic between each internally defined network security zone (i.e., internal sub-networks whose traffic is mediated by the firewall). This activity recognizes the pattern of common types of suspicious traffic that may indicate attempts by an internal user to access a specific computer for which the user is not authorized.

Server and workstation operating systems are updated with applicable security patches as they are made available by the vendors. Systems support staff subscribe to several nationally recognized security alert services to keep informed about current and emerging security issues or product vulnerabilities as they are made known. Procedures are in place for staff to respond to early warnings about security threats

whether during or outside regular business hours. Westat's response protocol includes immediate action to gather information, protect systems, inform users, and take any new protective measures, such as applying newly released security software updates.

Access to the local network from PC workstations is controlled through the use of login account passwords and screensavers that, once activated, require that the user's account password be re-entered before the PC can be used again. Passwords are initialized by the IT Manager, then encrypted and stored in protected files. The password encryption cannot be removed, and the password control system provides the following additional security features:

- A non-displaying/non-printing feature prevents the password from appearing on the workstation screen during the logon process.
- The system automatically limits the number of unsuccessful attempts to logon after which the account is disabled and must be reset by the system administrator.
- To ensure the confidentiality of passwords, users are required to change their passwords every 90 days.
- The system provides controls and is configured to ensure that each user has access to only the information for which he/she is authorized and has access to the minimum privileges necessary to perform his/her job.
- Accounts that have not been used for 90 days are automatically disabled and can be reactivated only by the system administrator. Otherwise, disabled accounts are deleted one week later.
- Passwords must be of a minimum length, must meet certain character rules and standards, and cannot be reused. Currently, Westat requires that network passwords have a minimum length of eight characters, to include at least three numeric, case change, or special ASCII characters (e.g., 0-9, &, %).

To protect PCs, email services, and network data storage facilities from damage caused by viruses and worms, Westat scans local PCs, network servers, and all email messages for possible viruses and worms. All networked PCs are required to use Westat-installed anti-virus software, which scans files for viruses before saving them to the network. All incoming and outgoing email is scanned, and any suspicious messages are quarantined for possible followup investigation. In addition, network disk storage areas are scanned in real-time mode and again once each night. The anti-virus scanning software is updated and distributed to network servers, email servers, and PCs automatically on a scheduled basis to ensure that currently reported viruses will be detected. Urgent updates can also be "pushed" to all servers and PCs between the scheduled times, when necessary to prevent the spread of a recently discovered virus.

When using the Internet or email services, staff are instructed to comply with Westat's "Electronic Mail and Internet Acceptable Use Policies and Guidelines." This document contains the policies and best practices for appropriate use of these resources.

4. IT Personnel Security

Qualified candidates for computer systems and programming staff positions are screened by management, and references are verified. In addition, Systems Support staff who are directly responsible for systems management and maintenance must undergo a criminal and driving record background check. Each Westat employee and contractor is instructed in Westat's data security polices, standards, and procedures through staff orientation programs and by the employee/contractor's manager/supervisor. Items covered include password administration, transmission or delivery of data files, and printing and handling of materials containing confidential data, such as field materials, reports, or frequencies. Employees are also instructed by their personnel supervisor or designee concerning policies and practices applicable to their particular assignments and at the time assignments change, in order to maintain security awareness. Westat's management structure also provides for separation of functions and responsibilities to limit any individual's access to and control of the data and the system. Westat policies, procedures, and memos are also available to all staff online on Westat's intranet ("WesInfo").

All Westat employees and contractors are required to read and pledge compliance with Westat's "Employee or Contractor's Assurance of Confidentiality of Survey Data." A thorough understanding and compliance with the terms of this confidentiality agreement are required of all Westat staff.

To ensure that data collected in projects are not available to anyone except authorized project personnel, a set of stringent confidentiality procedures are imposed on the field and telephone operations as well as on data processing:

- All employees sign an assurance of confidentiality.
- Employees are obligated to keep confidential all names and other personal data learned either incidentally or in the course of the data collection.
- A field worker or telephone interviewer may not knowingly collect data on a study subject he or she knows personally.
- Survey data are kept locked when not in use. Access is limited to authorized personnel.
- The project director is responsible for ensuring that Westat personnel and subcontractors are in compliance with all security procedures.

- The project director ensures that survey practices adhere to applicable contract provisions.

Data collection procedures, such as the assignment of study identification numbers to all subjects, are designed to guarantee confidentiality according to Federal regulations and any additional specific requirements of individual clients and contracts. Westat provides information for Special Agreement Checks (SAC), FBI fingerprint classifications, and name checks, as may be required under contract.

When a staff member leaves the company, appropriate steps are taken to transfer responsibility and preserve any data to which the user may have access. Terminating employees with certain access privileges may be given alternative assignments and their access privileges suspended upon notice of eventual termination. The day a staff member departs, his/her building access card is deactivated. Any computer accounts assigned to the user are deactivated to ensure that the departing employee no longer has access to project directories or network resources. If the staff member has a key to a secure room or a PC containing sensitive data, the locks are changed. The departing staff member is also reminded that he/she has signed the assurance of confidentiality agreement and remains bound to its terms and conditions.

5. Disaster Recovery

Westat has a formal disaster recovery plan to be used in the event of a significant failure of regular computing services due to fire, flood, long term power outage, or other events that have a major impact on systems operations. The plan identifies the primary and backup members of the disaster recovery assessment team and the functional systems area for which each person is responsible. If an event occurs that requires the attention of the team, all members assemble to begin an assessment of the situation for their respective area and prepare an estimate of the time and level of effort required to restore operations. Restoration efforts are directed by the team leader, who coordinates these activities with other senior corporate managers. Staff are to refer to the “Westat Computer Systems Disaster Recovery Plan” on WesInfo for additional information.

6. User Assistance and Incidence Reporting

User assistance for all aspects of Westat systems use can be requested by email, by telephone, or in person from Westat’s PC Helpdesk in the Office Automation Systems unit. A commercial call ticket and workorder tracking system is used to log all initial and followup contacts with users, to route calls to appropriate units, and to report to management on call activity. The PC Helpdesk will log the call and advise and assist the user in contacting the appropriate systems staff manager in the event that a call

pertains to project-specific systems for which the helpdesk does not have a service protocol. Reports of incidents requiring immediate attention, such as computer virus reports, are immediately addressed by the appropriate staff in the Office Automation Systems unit, which includes staff responsible for ongoing virus protection maintenance and for email system administration.

Any individual employed or contracted by Westat is encouraged to report any security incident or issue at any time to the appropriate manager, the PC Helpdesk, or the Human Resources Department. Staff are required to report security incidents in which they believe systems security has been, or may be, breached, such as by the unauthorized or suspicious presence of unidentified individuals on Westat premises; the unauthorized use of passwords; unauthorized access to a server area or otherwise secure systems area; the demonstrated or likely existence of a virus on a computer; and possible unauthorized transmission of confidential data without encryption or security.