Security for Information Technology Service Contracts

Julia Allen
Gary Ford
Barbara Fraser
John Kochmar
Suresh Konda
Derek Simmel
Networked Systems Survivability Program

Lisa Cunningham
Computer Sciences Corporation

January 1998

SECURITY IMPROVEMENT MODULE
CMU/SEI-SIM-003

Security Improvement Module

CMU/SEI-SIM-003
January 1998

Security for Information Technology Service Contracts

Julia Allen

Gary Ford

Barbara Fraser

John Kochmar

Suresh Konda

Derek Simmel

Networked Systems Survivability Program

Lisa Cunningham

Computer Sciences Corporation

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213

This report was prepared for the SEI Joint Program Office

HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

(signature on file)

Jay Alonis, Lt Col, USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-95-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

This document is available through Asset Source for Software Engineering Technology (ASSET): 1350 Earl L. Core Road; PO Box 3305; Morgantown, West Virginia 26505 / Phone: (304) 284-9000 or toll-free in the U.S. 1-800-547-8306 / FAX: (304) 284-9001 World Wide Web: http://www.asset.com / e-mail: sei@asset.com

Copies of this document are available through the National Technical Information Service (NTIS). For information on ordering, please contact NTIS directly: National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. Phone: (703) 487-4600.

This document is also available through the Defense Technical Information Center (DTIC). DTIC provides access to and transfer of scientific and technical information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. To obtain a copy, please contact DTIC directly: Defense Technical Information Center / Attn: BRR / 8725 John J. Kingman Road / Suite 0944 / Ft. Belvoir, VA 22060-6218 / Phone: (703) 767-8274 or toll-free in the U.S.: 1-800 225-3842.

Table of Contents

Preface

This document is one of a new series of publications of the Software Engineering Institute at Carnegie Mellon University—*security improvement modules*. They are intended to provide concrete, practical guidance that will help organizations improve the security of their networked computer systems.

Module structure

Each module addresses an important but relatively narrowly defined problem in network security. The first section of the module describes the problem and outlines a set of *security improvement practices* to help solve it. Each practice is a recommended way of performing common tasks related to the secure operation of networked computer systems.

The remaining sections of the module are detailed descriptions of the practices. Each includes a rationale for the recommended actions and a step-by-step description of how to perform them.

Intended audience

The practices are primarily written for system and network administrators within an organization. These are the people whose day-to-day activities include installation, configuration, and maintenance of the computers and networks. Occasionally, practices are also written to assist the managers responsible for network and system administration.

Revised versions

Network technologies continue to evolve rapidly, leading to both new solutions and new problems in security. We expect that modules and practices will need to be revised from time to time. To permit more timely publication of the most up-to-date versions, the modules and practices are also being published on the World Wide Web. At the end of each section of this document is the URL of its Web version.

Implementation details

How an organization adopts and implements the practices often depends on the specific networking and computing technologies it uses. For some practices, technology-specific implementation details have been written and are being published on the World Wide Web. The Web version of each practice contains links to the implementation details.

Acknowledgements

The authors would like to acknowledge the significant contributions of the reviewers of this module:

Joan Bonk

Bob Ellison

Steve Huth

Klaus-Peter Kossakowski

Mark Poepping

Security for Information Technology Service Contracts

An increasing number of organizations are contracting with outside companies for installation and maintenance of their information technology (IT). All too often, these organizations experience increased difficulty in providing appropriate oversight of the services and software for which they have contracted. For example, contractor access to the organization's systems is often neither well controlled nor secure, placing information systems and data at risk. The practices recommended below are designed to assist your organization in managing the contractor, managing the contract, and deterring common, known security problems when IT services and software are externally contracted.

Definitions

contractor services	all actions performed by the contractor on the software they are providing and for which your organization has contracted. These include, but are not limited to, installation, configuration management, development, update, test, maintenance, and operations.
contractor software	the code, data, and supporting documentation that the contractor delivers for installation and operation on your systems
information technology	software that operates in support of the day-to-day business and operations of your organization

Who should read these practices

These practices are applicable to your organization if you want to protect the confidentiality, availability, and integrity of your systems and data when you contract (or are planning to contract) with outside parties to install, configure, manage, and/or update any of your information technology. Examples of contracted services include Web site development and maintenance, installation and maintenance of electronic mail services, database management services, security services, or other network services.

These practices are intentionally independent of the software technology and services for which you have contracted. They may be used in conjunction with technology-specific practices such as those described in Security for a Public Web Site (CMU/SEI-SIM-002).

What these practices do not cover

These practices do not cover every aspect of security for IT service contracts. In particular, they do not address

- general contractor selection criteria and process. Practices related to security are addressed.
- relationships with resident contractors who are engaged in co-producing systems as a collaborative effort with your staff, i.e, operating in effect as full time employees
- any service contract that is executed in total as physically separate from your facility and systems with no remote access or onsite connection
- outsourcing of the entire IT function including movement of your organization's IT employees to the outside company
- the details of any specific information technology

Security issues

There are three main security issues related to security for IT service contracts:

1. The contractor's security policies and practices might not be adequate when compared to those of your organization. This can result in
   - undetected intrusions or security violations due to insufficient auditing and monitoring policies on the contractor's part
   - lack of predictable data and configuration integrity due to a mismatch between your and your contractor's separation of duty policy (clear assignment of roles and responsibilities) or your and your contractor's redundancy policy (having sufficient checks and balances to ensure an operation is done consistently and correctly)
   - loss of privacy due to the contractor handling your sensitive information in a less rigorous fashion that your organization's policy dictates
2. Your systems might experience loss of confidentiality and integrity by virtue of the contractor using an unsecure method of remote access. This may result in intruders from either the contractor's organization or elsewhere
   - gaining unauthorized access to, modifying, or destroying your organization's information systems and assets
   - deliberately introducing security vulnerabilities, Trojan horses, or viruses
   - launching attacks on other systems from your network and perhaps making your organization liable for damages
3. Your systems might experience loss of availability when contractor access occurs. This may result in conflict for key resources that are required for critical in-house operations when contractor processing occurs at the same time as these operations causing a denial of service condition.

Security improvement approach

To improve the security of IT service contracts, we recommend a three-step approach. It requires implementing security practices in these areas:

1. *preparing* for contracted IT services
2. *managing* contracted IT services
3. *concluding* contracted IT services

Summary of recommended practices

Area	Recommended Practice
Preparing for contracted IT services	1. Specify security requirements and assess contractor capability. 2. Determine contractor ability to comply with your organization's security policy.
Managing contracted IT services	3. Require that the contractor software is installed and configured to operate securely. 4. Require that the contractor communicate securely with your site when operating remotely. 5. Control contractor access to your systems. 6. Look for unexpected changes to directories and files. 7. Inspect your system and network logs. 8. Review contractor performance.
Concluding contracted IT services	9. Eliminate physical and electronic access by the contractor to your systems and networks.

Abbreviations used in these practices

CBC	cipher block chaining
DES	Data Encryption Standard
DNS	Domain Name Service
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
IT	information technology
MIME	Multipurpose Internet Mail Extension
PGP	Pretty Good Privacy
RC2/5	block cipher variable-key-length algorithms developed by Rivest
RSA	Rivest, Shamir, and Adleman (inventors of RSA encryption system)

References and sources

[Maximum 97] *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*. Indianapolis, IN: Sams.net Publishing, 1997.

[Atkinson 97] Atkinson, Randall J. "Toward a More Secure Internet." *IEEE Computer 30*, 1 (Jan. 1997): 57-61.

[Firth 97] Firth, Robert, et al. *Security for a Public Web Site*. (CMU/SEI-SIM-002, ADA329626). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997.

[IETF 97] Internet Engineering Task Force Network Working Group. *RFC 2196 Site Security Handbook* [online]. Edited by Barbara Fraser. Available FTP: <URL: ftp://ds.internic.net/rfc/rfc2196.txt> (1997).

[Summers 97] Summers, Rita C. *Secure Computing*. New York, NY: McGraw-Hill, 1997.

Where to find updates

The latest version of this module is available on the Web at URL

`http://www.cert.org/security-improvement/modules/m03.html`

1 *Specify security requirements and assess contractor capability.*

It is common to specify requirements for functionality, price, performance, and capacity when selecting externally-provided information technology services. When you specify the requirements for selecting such services (including hardware, operating system, software, and data), you should also include security requirements for the technology and for the activities of those who will install, configure, maintain, and dispose of it. Once these requirements are clearly specified, you need to ensure that any outside contractor you select has the ability to meet these requirements.

This practice assumes that you have made a business decision to contract with an outside company for a specific information technology service and are in the process of selecting that company.

Why this is important

Many companies provide information technology software and supporting services. These companies and the software and services they provide vary with respect to their ability to meet your organization's confidentiality, availability, and integrity requirements. Therefore, it is critical that you clearly specify your security requirements and require candidate contractors to demonstrate their ability to meet these requirements. You should also gather independent evidence of each candidate contractor's track record with respect to security. This will help to ensure that the contractor you select is capable of operating in a manner consistent with your security requirements.

How to do it

There is some repetition in the "How to do it" steps for this practice and the following practice. For the purpose of future practice development, we have chosen to separate the topics of security requirements and security policy even though, for some audiences, these have a high degree of overlap.

➤ *Identify technology security requirements.*

Based on your organization's security needs, identify specific security-related requirements for the technology for which you are contracting. General, technology-related requirements might include lack of vulnerability to known forms of attack against the technology, the ability to restrict systems administrator-level access to authorized users, support for your specified user authentication technologies (e.g., one-time passwords), and the ability to log appropriate activities for purposes of detecting intrusions and attempted intrusions.

- *Identify security requirements that the contractor must meet in addition to those related to the specific technology.*

  These might include the method of remote or onsite access, managing such access (including the identification of an emergency point of contact), technology installation and maintenance, access and removal of access to facilities and systems, contractor liability, including warranting that no Trojan horses or viruses exist in contractor software, and having recently completed a security evaluation encompassing the technology being selected.

- *Include all security requirements in the solicitation for outside bids.*

- *Assess the contractor's capability to meet your security requirements.*

  Request references for other customers of the contractor and conduct an interview with those customers to assess their level of satisfaction with the contractor's ability to meet security requirements. Require that the contractor demonstrate the required capabilities for and approach to security enforcement. Optionally, conduct a tailored security evaluation of a contractor's installation of the specified technology.

- *Write the security requirements into the contract work statement. Include explicit procedures where necessary.*

- *Execute a non-disclosure agreement if one is not already in place.*

  This is recommended in those cases where your contractor may encounter proprietary information on your systems.

Other information

We recommend that your organization's purchasing guidelines mandate the specification of security requirements for all information technologies.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p018.html`

2 *Determine contractor ability to comply with your organization's security policy.*

A security policy defines the set of laws, rules, and practices that regulate how an organization implements, manages, protects, and distributes computing resources to achieve security objectives. One of the policy's primary purposes is to define the range of threats that your organization chooses to guard against and how these threats are dealt with when manifested.

Contractors are responsible for understanding and respecting your security policy when they are connected to your systems. They must comply with stated practices, using resources only for the approved purposes of the organization, and only in the authorized ways.

This practice assumes that your organization has defined and implemented a security policy reflective of your business objectives.

Why this is important

The purpose of having contractor practices that are compatible with your security policy is to protect your computing assets from undesirable outside access, threats, and vulnerabilities introduced by contractor access and delivery of service.

How to do it

There is some repetition in the "How to do it" steps for this practice and the previous practice. For the purpose of future practice development, we have chosen to separate the topics of security requirements and security policy even though, for some audiences, these are considered to have a high degree of overlap.

➤ *Examine your organization's security policy and determine the applicability of each section to this contract.*

Candidate areas to consider include privacy (monitoring of electronic mail, access to files), access (acceptable use guidelines for users), accountability (responsibilities of users, auditing, incident handling), authentication (passwords, remote location), availability of resources (redundancy and recovery), system and network maintenance (ability to perform remote maintenance), and violations/incidents (what is to be reported and to whom). (See also the *IETF Site Security Handbook, RFC 2196*, [IETF 97])

➤ *Communicate your policy to your contractor.*

➤ *Ensure that your contractor accepts your policy. Write this into the contract terms and conditions and/or contract work statement.*

➤ *Require that your contractor demonstrate the ability to comply with your policy.*

Request references for other customers of the contractor and conduct an interview with those customers to assess their level of satisfaction with the contractor's ability to comply with security policy. Require that the contractor demonstrate the required capabilities for and approach to security policy enforcement.

Policy considerations

Your organization's information technology security policy should

- include language that constrains access to only the organizational information that is specifically required by an outside contractor to perform contracted services and prohibits access to all other information. The penalties for violating specified constraints should also be addressed (e.g., contract termination).
- address how your organization's information is handled and protected at the contractor's facility/site

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p019.html`

3 *Require that the contractor software is installed and configured to operate securely.*

Contractor software must be configured and installed so that its installation and use do not compromise the security of your systems. Contractor software should be checked by your system administrator to ensure that it is intact as the contractor originally intended.

Prior to installation, you are normally presented with a number of choices for configuration options or preferences. These choices should be made carefully by your contractor and system administrator to adhere to your security policy and balance your security and operational requirements.

Why this is important

It is critical to ensure that the contractor software is installed securely to protect both the newly installed software and your existing systems. As a result of installation, the complete software configuration must be documented and archived to establish a configuration management baseline. If the initial and subsequent installations are not properly baselined, there is no way to explicitly determine expected content, data, functionality, performance, or compliance with security requirements. Tracking changes to the baseline and any impacts resulting from those changes will not be possible.

In addition, making informed decisions about configuration details (as opposed to automatically accepting the default settings) will support you in determining expected states of operation and will facilitate problem identification and solution formulation. Default settings can often change from version to version; if you rely upon default settings, what may have been installed securely in the initial version may not be installed securely in any subsequent version.

How to do it

➤ *Make any necessary preparations to receive the contractor software.*

This includes reserving appropriate computing and storage resources and conveying any configuration or operational constraints to the contractor. Carefully address the effects of any changes that must be made to your organization's configuration of operational networks and systems to accommodate the contractor's software.

This step also includes limiting contractor access to only those portions of your networks and systems that are required for installation, assuming that the contractor is performing the installation. Consider logically or physically isolating the installation process and software to be installed.

Ensure that you have a way to return to the system and software configuration that existed prior to the installation of the contractor's software if there are problems with that software. A candidate procedure would be to perform a system backup, install the contractor software, and test the contractor software. If the test fails, uninstall the contractor software and restore your system to a known, previous state (represented by the backup). If the test succeeds, establish a new configuration and perform a new system backup.

➤ *Document the contractor software configuration to be installed.*

This includes the source of the software (e. g., contractor organization, system, network, server, versions), date of configuration, responsible parties, approval signatures, and a test summary demonstrating that the installed configuration provides the agreed-to capabilities. The configurations to be recorded include all software modules (source and object) and cryptographic checksums from both the contractor site and your site, documentation, development tools, configuration management tools, and test cases used to demonstrate a successful installation.

➤ *Create and record cryptographic checksums of the installed software.*

Create and record cryptographic checksums or other integrity-checking baseline information both before installation and after all installation and configuration choices have been made and installation has been successfully accomplished. You will use this information to periodically reverify the installed software, configuration, and date (notion of authoritative reference data for integrity checking).

Checksums should be kept on a separate server or a separate medium that is accessible only by trusted users. You might also consider the use of integrity-checiing tools such as Tripwire for the generation and subsequent checking of digital signatures for all files.

➤ *Verify the authenticity of the software being installed.*

Compare the installed configuration with the contractor's delivered configuration. This can be accomplished by the use of cryptographic checksums or a direct comparison with a known, trusted version of the software in combination with change detection (which detects changes to file attributes such as permissions, ownerships, modification time, and checksums as well as detecting new and missing files).

Ensure that no Trojan horses or viruses exist in the contractor software. Unix-based file- and system-integrity checking tools are available (e.g., Tripwire) as are virus scanners for PC-based systems.

➤ *Configure the contractor software to operate securely.*

Default configuration settings are often optimized to achieve the most desirable performance. Satisfying security requirements will usually necessitate a different configuration. Failure to change from the default or preferred config-

uration will likely make the contractor software, and potentially other related systems and software, vulnerable to attack. Ensure the contractor pays particular attention to configuration settings for logging and access control.

Evaluate the features of the technology being installed and its operational environment to assist in performing this step. For example, for Unix and Windows NT, grant the least privilege/access required to perform the installation.

➤ *To the extent possible, ensure the contractor thoroughly tests their software in a non-production environment prior to moving the software into your operational systems.*

➤ *If the installation must be performed remotely from your facility and network, ensure that all communications are performed securely.*

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p020.html`

4 *Require that the contractor communicate securely with your site when operating remotely.*

It is increasingly common for organizations to provide their contractors with the ability to remotely access hosts on the organization's internal networks. If this is the case for your contractor, you must establish policies and procedures for secure communications. In addition, you must implement technologies that provide strong authentication and secure communications between hosts, particularly when the remote connection takes place over any network that is not completely under your organization's control, e.g., the contractor logs into your internal hosts via the Internet or uses dial-in access via the public telephone network.

Why this is important

Commonly used applications transmit data between hosts in clear text, i.e, unencrypted. Without additional security measures, these data may be intercepted during transit, thus providing the interceptor a verbatim record of the data as it travels over the network between the hosts. As a result, the security risks that may arise include

- *Unauthorized access*. Information about users, authentication processes, and host and network configurations intercepted in transit may be employed by intruders to gain unauthorized access to your organization's internal networks. Successful attacks against your organization's internal networks may lead to the capture, modification, and destruction of data. Compromised systems may subsequently be subverted by intruders to launch attacks against other internal and external systems.
- *Loss of confidentiality*. Interception of sensitive data may include passwords and the contents of sensitive documents exchanged between the communicating hosts. Compromised information may subsequently be inappropriately disclosed, abused to misrepresent your organization, or used to execute an attack on your organization.
- *Denial of service*. Information about applications and host and network configurations intercepted during transit may be employed by attackers to bombard, divert, or block your organization's network services, thereby denying access to those services by authorized users.

You must assume that the contractor's network, software, and their access to your networks and systems may be compromised and, as a result, you must protect your assets accordingly.

How to do it

➤ *Authenticate the communicating hosts.*

Use a strong public key (asymmetric) encryption method such as RSA to authenticate all connections between hosts.

As examples, RSA is implemented within Secure Shell (ssh) and PGP. The Kerberos authentication system provides both client/server and user authentication. It is available for both the Unix and PC environments.

Provide the required authentication technology and keys to the contractor. Do *not* rely on IP addresses and Domain Name Service (DNS) for authentication of hosts over insecure channels. Using certain operating system mechanisms (e.g., *.rhosts* and *hosts.equiv* in Unix) can make your connection susceptible to IP and DNS spoofing.

➤ *Authenticate the external (contractor) user.*

If possible, use a strong public key method to authenticate the external user. If not, a range of other technologies can be employed. These include one-time passwords, a cryptographic challenge-response protocol, or a token device such as a smart card.

➤ *Upon successful authentication, encrypt all subsequent communications between hosts and users for the exchange of sensitive information.*

Use strong block-cipher technologies such as DES (CBC mode), Triple-DES, IDEA, Blowfish, RC2, or RC5 to secure communications between hosts. Private key block-cipher technologies are much faster for bulk encryption of data than public key.

Consider ssh or secure Telnet for conducting a secure session.

Consider PGP or Secure MIME for the exchange of electronic mail and files.

➤ *Document, monitor, and reset connection states.*

Data to be documented should include the remote host name and address, the method used for host and user authentication, user id, time of connection start and end, connection status, and specific circumstance by which a connection was lost, if possible.

The state of all active connections (dialup or direct) should be monitored and, upon failure or disconnect, be immediately terminated and reset. Modems and other applicable intermediate devices and software should also be reset automatically upon loss of connection to prevent hijacking of those connections.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p021.html`

5 *Control contractor access to your systems.*

You have several decisions to make related to providing contractor access to your organization's systems, e. g., when, for how long, and for what purpose. The contractor should be granted access only as needed to perform their contracted services. This access needs to be strictly controlled and enforced. You should also apply the principles of least privilege (contractor access to resources should be authorized only for the resources required to perform the task) and timely revocation of trust (contractor access to resources should persist only as long as needed to perform the task).

Why this is important

Outside access to your systems can interfere with your business-critical processing if it is not carefully managed and controlled. Understanding what is going to be done during the time that the contractor is accessing your systems will permit you to identify potential problems resulting from resource conflicts and to schedule such access to minimize interruptions to your normal operations.

If the contractor is accessing your systems remotely, you must assume that the contractor's network, software, and their access to your networks and systems may be compromised. This includes assuming that any member of the contractor's staff can try to access your organization's systems and data at any time that they choose, with or without your knowledge. You want to minimize the length of time that the contractor is remotely connected to your systems to minimize this risk.

How to do it

When contractor processing can be explicitly scheduled

To the extent possible, isolate the contractor hosts and software from the rest of your network. This can be accomplished via a range of solutions including using a separate subnet, filters, or a firewall to restrict traffic.

- *Require that the contractor notify you in advance when access is needed.*
- *Require that the contractor describe exactly what actions will be taken when they access your system.*

To effectively prepare for such access, you need a very good understanding of the tasks being performed and their ramifications. This can be accomplished through the use of checklists.

➤ *Analyze the impact of the task on other business-critical functions.*

Reschedule or disallow access if the contractor task interferes with those functions.

While it is expected that availability may be affected when contractor software upgrades are being installed, ensure that contractor activities will not create an extended denial of service condition, i.e., minimize the downtime of any business-critical functions. This can be accomplished by scheduling this task to occur during off hours.

➤ *Allow contractor connectivity to your systems only when a scheduled task is to be performed. Disable access at other times.*

When contractor processing must occur 24 hours a day or in an emergency

➤ *Establish pre-arranged procedures for 24-hour and emergency access as part of contract negotiations.*

An example of such a procedure would be for the contractor to notify the on-call system administrator to arrange access prior to performing the service. The system administrator would be responsible for monitoring access and examining all relevant logs.

An alternate example would be for the contractor to perform the service and then call the system administrator immediately (or in parallel).

Decisions to be made as part of these procedures include

- when and under what conditions your system administrator notifies the contractor
- when and under what conditions the contractor notifies your system administrator
- access procedures and limitations
- the means for enabling recording of all events, activities, changes, decisions, results, etc.

Policy considerations

Your organization's information technology security policy should

- include language that constrains access to only that organizational information that is specifically required by an outside contractor to perform contracted services and prohibits access to all other information. The penalties for violating specified constraints should also be addressed (e.g., contract termination).

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p022.html`

6 *Look for unexpected changes to directories and files.*

It is critical that you actively monitor contractor access to and processing on your systems and networks including the examination of all relevant directories and files. The file systems in your network environment contain a variety of software and data files. Unexpected changes in directories and files, especially those to which access is normally restricted, may be an indication that an intrusion has occurred. Changes may include modifying, creating, or deleting directories and files. What makes such changes *unexpected* may depend on who changed them and where, when, and how the changes were made.

Why this is important

Intruders often substitute, modify, and damage files on systems to which they have gained access. To hide their presence on your systems, it is common for intruders to replace system programs with substitutes that perform the same functions but exclude information that could reveal their illicit activities. They also often modify system log files to remove traces of their activities. By masking their presence on a compromised system, intruders prolong the time they have to use that system for their purposes. In several notable cases, the presence of intruders on compromised systems was not discovered until many months after the initial intrusion occurred.

Intruders may also create new files on your systems. For example, they may install *backdoor* programs or tools used to gain privileged access on the system. Intruders also make use of the disk space on compromised systems to store their tools and contraband.

Private data files and files containing mission-critical information are common targets of modification or corruption by intruders. Information about your organization that is accessible to the public or to subscribers via public networks and the Internet is also a common target. Several documented cases exist of prominent organizations that have had their Web sites modified to include offensive content and other erroneous information.

How to do it

➤ *Establish priorities and schedules.*

Examine the files on your system and prioritize the frequency with which they should be checked. The more mission- or security-critical the file, the more frequent the checking should be.

➤ *Maintain authoritative reference data for critical files and directories.*

For each file and directory, the authoritative reference data you maintain should provide enough information for you to be able to identify changes to

- location in the file system
- alternate paths to it, via links, aliases, or shortcuts
- contents of files, entries in directories
- exact size, and if possible, file system units allocated
- time and date indicating when the file or directory was created and last modified
- ownership and access permission settings, including execution privilege settings for software

Use robust cryptographic checksum technologies to generate a checksum for each file. Keep authoritative copies of files and checksums on write-protected or read-only media stored in a physically secure location.

➤ *Verify the integrity of directories and files according to your established schedule.*

Compare the attributes and contents of files and directories to the authoritative reference (either complete copies or cryptographic checksums). Identify any files and directories whose contents or other attributes have changed.

Always access authoritative reference information directly from its secured, read-only media. Never transmit authoritative reference information over unsecured network connections.

➤ *Identify any missing files or directories.*

➤ *Identify any new files and directories.*

Pay special attention to any new program files and their associated execution privilege settings.

➤ *Investigate any unexpected changes among those you have identified.*

If any changes cannot be attributed to authorized activity, initiate your intrusion-response procedures immediately.

Report the incident to your organization's designated security point of contact.

Policy considerations

Your organization's networked systems security policy should

- Define the responsibilities and authority of systems administrators and security personnel to examine file systems on a regular basis for unexpected changes. Users should be told about such authority and examination.
- Require users to report any unexpected changes to their software and data files to system administrators or your organization's designated security point of contact.

Other information

As authorized and expected changes are made to files and directories, you will need to perform your organization's procedures for securely updating your authoritative reference data.

Some kinds of important files are expected to change frequently (perhaps several times per second); these include system log files, transaction log files, and database tables. In general, the techniques described above will not be particularly useful in distinguishing normal changes to such files from those that might have been caused by intruders. Techniques based on transaction auditing are more useful in these cases.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p002.html`

7 *Inspect your system and network logs.*

It is critical that you actively monitor contractor access to and processing on your systems and networks including the examination of all relevant system and network logs. Frequently, intruders leave traces of their actions in system log files. Hence, checking system and network log files periodically is one way to detect intrusions.

Why this is important

Logs may contain evidence of unusual and unexpected activities that have occurred on the system or network. Such log entries may indicate that someone has compromised or tried to compromise the system. By looking at log files on a regular basis, you may be able to identify attempted or successful intrusions soon after they occur and initiate the proper damage-prevention or containment procedures.

Background information

Log files vary depending on the operating system, application software running on the system, and logging configuration you have chosen. Multiuser operating systems often provide more extensive logging capabilities than do single-user operating systems. Table 1 describes information typically contained in logs.

Type of Log	Information Contained in the Log
user activity	• login activity • changes in user identity • file accesses by the user • authorization information • authentication information
process activity	• commands run by users • running-process information including program name, user, start and stop times, and execution parameters
system activity	• restarts and shutdowns of the system • administrative logins
network connections	• details (when, where, what kind) of connections attempted or established with the system • details of connections established from the system
network traffic monitoring	• records of all network traffic transactions

How to do it

➤ *Periodically inspect each type of log file.*

We recommend that each log file be inspected at least daily.

Look for evidence of unusual or unexpected activity. One benefit of periodic inspections is that, over time, you will become increasingly familiar with the signs of *usual* and *expected* activity. This will make it easier to recognize the unusual and unexpected.

The table below summarizes unusual or unexpected activities that may be reported in each log type. For operating systems that support different levels of user privilege, be sure to look for unusual activity by users at all levels.

Type of Log	Unusual or Unexpected Activities
user activity	• repeated failed login attempts • logins from unexpected locations • logins at unusual times of day • unusual attempts to change user identity • unusual processes run by users • unauthorized attempts to access restricted files
process activity	• processes that are run at unexpected times • processes that have terminated prematurely • unusual processes (i.e., those not due to normal, authorized activities)
system activity	• unexpected shutdowns • unexpected reboots
network connections	• connections to or from unusual locations • repeated failed connection attempts and their origination and destination addresses and ports • connections made at unusual times • unexpected network traffic (i.e., contrary to your firewall configuration or unexpected traffic volume)
network traffic monitoring	• sweeps of your network address space for various services, indicating attempts to identify hosts on your network and the services they run • repeated half-open connections (may signify IP spoofing attempts, or denial of service activity) • successive attempts to connect to unusual services on your network's hosts • transactions originating outside your network with destinations also outside your network (signifying traffic that should not be traversing your network) • sequential (attempted) connections to specific services signifying someone trying to run network-probing tools against your networked systems

➤ *Document any unusual entries that you discover.*

Over time, you may see recurring kinds of unusual log file entries. Maintaining records of such entries and what you determined to be their causes will help you and others to understand new occurrences more quickly and accurately.

➤ *Investigate each documented abnormality.*

Ask yourself questions such as

- Can it be explained by the activities of an authorized user? (e.g., the user really was in Cairo last week and connected to the network)
- Can it be explained by known system activity? (e.g., there was a power outage that caused the system to reboot)
- Can it be explained by authorized changes to programs? (e.g., the mail log showed abnormal behavior because the system programmer made a mistake when the software was modified)

➤ *Report all confirmed evidences of intrusion (or attempted intrusion) to your organization's internal security point of contact.*

➤ *Read security bulletins from trustworthy sources (e.g., CERT® advisories and summaries[1]) and other security publications regularly.*

This can increase your understanding of current intruder activities and methods, and you can use this information to improve what you look for in log files.

Policy considerations

Your organization's networked systems security policy should:

- Specify that log files be inspected on a regular basis by authorized personnel, and that anomalies be recorded and reported to your organization's designated security point of contact.

Other information

If your site has large networks of systems with many log files to inspect, consider using tools that collect and consolidate log file information. Over time, you will learn what is normal for your environment. You should integrate this knowledge into your site's specific procedures for inspecting log files.

Also, as you acquire, modify, or retire systems, your log review procedures may need to change. Make sure that your site's procedures are appropriate for your current technology.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p003.html`

1. See http://www.cert.org and ftp://info.cert.org/pub/cert_advisories/ .

8 *Review contractor performance.*

During the course of a contracted relationship, your organization's network or system administrators must review the operation and security performance of the contractor software. In addition, they should review contractor practices and procedures to ensure continued compliance with security policy and requirements established at the initiation of the contract.

You must establish a process for addressing and resolving user problem reports against the contractor software as well as the review of pertinent information in the event of unscheduled or emergency access. This practice assumes such a problem reporting process exists and is being followed.

Why this is important

It is important that contractor compliance with your security requirements and policy is tracked against original commitments. Corrective actions must be taken immediately when contractor performance deviates from the original plan. Opportunities must be created to negotiate changes to commitments when required. It is critical that corrective actions are captured as part of a well-defined problem-reporting process that tracks a problem actively from initiation to closure. Regular review can serve as a proactive, preventive, visible step to keep the relationship between you and your contractor on track and ensure that the services being provided are as agreed and expected.

How to do it

For ongoing review

These steps assume that review of contractor performance is performed either on a regular basis, e.g., quarterly, or as driven by events, e.g., software installation or major upgrade.

➤ *Establish a process for reviewing contractor compliance with specified security requirements.*

General, technology-related requirements might include lack of vulnerability to known forms of attack against the technology, the ability to restrict systems administrator-level access to authorized users, support for your specified user authentication technologies (e.g., one-time passwords), and the ability to log appropriate activities for purposes of detecting intrusions and attempted intrusions.

Security requirements that the contractor must meet in addition to those related to the specific technology might include the method of remote or onsite access, managing such access (including the identification of an emergency

point of contact), technology installation and maintenance, and access and removal of access to facilities and systems.

Specific security requirements are contained in the contract work statement.

➤ *Establish a process for reviewing contractor compliance with your security policy.*

Candidate policy topics might include privacy (monitoring of electronic mail, access to files), access (acceptable use guidelines for users), accountability (responsibilities of users, auditing, incident handling), authentication (passwords, remote location), availability of resources (redundancy and recovery), system and network maintenance (ability to perform remote maintenance), and violations/incidents (what is to be reported and to whom). (See also *IETF Site Security Handbook, RFC 2196*, [IETF 97])

Specific policy statements are contained in the contract terms and conditions and/or contract work statement.

➤ *Conduct periodic reviews to verify contractor compliance.*

Require that the contractor demonstrate that major software upgrades were done correctly, in accordance with security policies, practices, and processes. Require that the contractor verify that no other operational systems have been negatively affected by the upgrades. This can be accomplished through the examination of all relevant logs.

➤ *Regularly execute a file system integrity-checking tool.*

As an example, Tripwire will tell you about the state of the collection of files on your system (added/deleted), changes in state (protection changes), and changes to file contents. Executing Tripwire daily will provide timely notification of problems, thus resulting in more timely correction.

➤ *Ensure that no Trojan horses or viruses exist in the contractor software.*

This can be accomplished by a comparison of cryptographic checksums with a prior, trusted version of the software if such a trusted version exists. Other (primarily Unix) file- and system-integrity checking tools are also available (e.g., TripWire) as are virus scanners for PC-based systems.

➤ *Review user problem reports.*

During this review, identify any recurring trends, bring these to the contractor's attention, and request an action plan to resolve the problem.

For emergency access

➤ *Upon unscheduled or emergency access of your systems by the contractor, conduct an immediate review of pertinent logs if this is not performed automatically.*

➤ *Perform a post-mortem review with the contractor to determine the cause of the emergency and discuss how to avoid this in the future.*

Policy considerations

Your organization's information technology security policy should:

- include language that constrains access to only that organizational information that is specifically required by an outside contractor to perform contracted services and prohibits access to all other information. The penalties for violating specified constraints should also be addressed (e.g., contract termination).

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p023.html`

9 *Eliminate physical and electronic access by the contractor to your systems and networks.*

Once the contractor has fulfilled their contract with your organization and completed all services, there is no further need for the contractor to have access to your facilities, systems, and data. It is essential that you capture the final state of the contractor software configuration and remove all opportunities for the contractor to access your systems.

Why this is important

In maintaining a secure system, you must ensure that only authorized users have access to that system. Otherwise, you run the risk of unauthorized access to systems, data, and proprietary information, e.g., the contractor could remotely disable the software they installed on your systems in the event of some grievance or dispute.

Capturing the final state of the contractor software configuration is critical in the event that future problems, claims, or disputes arise, i.e., you want to ensure that you are able to identify the configuration content and capabilities as they were delivered to your organization.

How to do it

➤ *Eliminate contractor physical access to your facilities.*

How you do this depends on the methods your organization uses to control access to your physical facilities. This could include the return of badges and access cards, removal of contractor staff names from reception area access lists, and notifying your staff that the contractor is no longer working with your organization.

➤ *Remove contractor authentication and all means of access to your systems.*

Ensure that you have a complete list of all contractor user IDs, passwords, and cryptographic keys. Eliminate these from all authentication processes. In addition, eliminate all contractor host access mechanisms. These may include open ports in router configurations, host service configurations, and host-to-host authentication keys.

If contractor user IDs are necessary to continue operating the software as they have installed and delivered it, it will suffice to change all contractor passwords to prevent further access by their staff. As a general rule, do not reuse contractor IDs once they have been retired.

➤ *Archive the contractor software configuration.*

Capture the configuration of all software, data, documentation, and supporting information. This includes the source of the software (e. g., contractor organization, system, network, server, versions), date of configuration, responsible parties, approval signatures, and a test summary demonstrating that the final configuration provides the agreed-to capabilities. The configurations to be recorded include all software modules (source and object) and their cryptographic checksums, documentation, development tools, configuration management tools, and test cases used to demonstrate agreed-to capabilities.

Archive this configuration in a secure manner. This may include retaining a copy offsite from your facility and systems or using other means that you have implemented for disaster recovery.

➤ *Transfer responsibility, authority, and ownership for the contractor software.*

Transfer responsibility, authority, and ownership for the operation and maintenance of all contractor software to designated internal staff. Include all contractor files and supporting data. No files should remain "owned" by the contractor's user IDs on your systems. After making a complete backup of all contractor files, change the ownership of all such files to your internal staff. This assumes that operation of the contractor software is not dependent upon the use of explicit contractor IDs.

➤ *Ensure that non-disclosure agreements executed at contract initiation are still in effect.*

➤ *Require that the contractor sign a statement warranting that no Trojan horses or viruses exist in their software.*

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p024.html`

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 1998	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Security for Information Technology Service Contracts	C — F19628-95-C-0003

6. AUTHOR(S)

Julia Allen, Lisa Cunningham, Gary Ford, Barbara Fraser, John Kochmar, Suresh Konda, Derek Simmel

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-SIM-003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/AXS
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12.a DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12.b DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

An increasing number of organizations are contracting with outside companies for installation and maintenance of their information technology (IT). All too often, these organizations experience increased difficulty in providing appropriate oversight of the services and software for which they have contracted. For example, contractor access to the organization's systems is often neither well controlled nor secure, placing information systems and data at risk. The practices recommended in this document are designed to assist your organization in managing the contractor, managing the contract, and deterring common, known security problems when IT services and software are externally contracted.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information technology security, information technology services, information technology software, remote system access, software outsourcing	30
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL