



TMCC

**Truckee Meadows
Community College**

Information Technology Operations

**COMPUTER SECURITY
INCIDENT ACTION PROCEDURES**

TABLE OF CONTENTS

Roles and Responsibilities.....	3
Users.....	3
Managers.....	3
System Administrators.....	3
Computer Incident Response Team (CIRT).....	3
TMCC Police Department.....	3
Public Information Office (PIO).....	4
Threat Environment	5
Internal and External Threat	5
Internal Threat.....	5
External Threat	5
Malicious Code Attacks.....	5
Virus Incidents	5
Macro Viruses.....	6
Worms	6
Trojan Horses.....	6
Modem Dial-in.....	7
Suspected Cracker or Hacker Compromise.....	7
Cracker or Hacker Activity Eradication.....	7
Technical Vulnerabilities	8
Procedures for Responding to Incidents	9
Preparation	9
Baseline Protection	9
Planning and Guidance	9
Training.....	9
Identification	10
Determine the Symptoms	10
Identify the Nature of the Incident.....	10
Identify the Evidence	11
Protecting the Evidence.....	11
Report the Events.....	11
Containment.....	11
Maintain a Low Profile	12
Avoid Potentially Compromised Code.....	12
Back up the System.....	12
Change Passwords.....	12
Eradication.....	12
Determine the Cause and Symptoms	13
Improve Defenses.....	13
Perform Vulnerability Analysis	13
Recovery.....	13
Determine the Course of Action	13
Monitor and Validate System.....	13
Follow-up.....	13

Document Response Quality to Incident.....	14
Document Incident Costs.....	14
Preparing a Report.....	14
Revising Policies and Procedures.....	14
Notification.....	14
Conclusion	15
Glossary.....	16

ROLES AND RESPONSIBILITIES

Each Truckee Meadows Community College (TMCC) staff member, from end users of the TMCC network resources to the President's office, has responsibilities related to the security of TMCC's computing systems.

Users

Computer users may be the first to discover an intrusion. Both end users and system users need to be vigilant for unusual system behavior, which may indicate a security incident in progress. In addition to their incident reporting responsibilities, system users may at some point be responsible for reporting incidents (e.g., a virus infection, a system compromise, or a denial of service incident, which is detected by resident software on the system user's workstation) to the Information Technology Operations (ITO) Help Desk.

Managers

Managers ensure that their employees are aware of the reporting procedures and the security policies in place to protect TMCC information systems, employees, and property. They are responsible for reporting security incidents to the ITO Help Desk. The ITO Help Desk will inform TMCC's IT Management of the incident.

System Administrators

System administrators, familiar with TMCC systems, may often be the first to discover a security incident. Like managers, system administrators are responsible for immediately reporting these incidents to IT Management. Additionally, they may be called upon to help determine and implement a solution, when applicable.

Computer Incident Response Team (CIRT)

TMCC's IT Management has established the TMCC CIRT. The CIRT is the college's action team designed to assist of behalf of the TMCC IT departments in handling security incidents. CIRT responsibilities include discovery of and response to, activities which might otherwise interrupt the day-to-day operations of the TMCC computer infrastructure. Furthermore, the CIRT is established to formalize reporting of incidents and disseminating incident information with TMCC community.

TMCC Police Department

The TMCC Police Department provides law enforcement authority and investigative support to any incident handling initiatives. If criminal activity is suspected, the TMCC Police Department must be notified immediately. As determined by the TMCC Police Department, other law enforcement support may be called in to assist in the investigation of an incident.

Public Information Office (PIO)

The PIO is responsible for answering questions from the public regarding activities with TMCC. When a computer security-related incident occurs, the PIO may disseminate information, if needed, to the public. TMCC employees are not authorized to disseminate information related to computer security incident to the public (including the media), but should work to provide such information to IT Management who will coordinate with the PIO.

THREAT ENVIRONMENT

Although computer security incidents may take many forms and involve many devious means, there are certain types of attacks which occur more frequently than others. Knowing what these types of attacks are and how TMCC counters them will help TMCC staff be best prepared to react and report all related information to the ITO Help Desk.

Internal and External Threat

Internal Threat

An internal threat is any instance of a user misusing resources, running malicious code, attempting to gain unauthorized access to an application, or anything that may cause a denial of service. Examples include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data. More significant internal threats may include an otherwise authorized system administrator who performs unauthorized actions on a system.

External Threat

An external threat is any instance of an unauthorized person attempting to gain access to systems or cause a disruption of service. Examples include disruption/denial of service attacks, mail spamming, and execution of malicious code that destroy data or corrupt a system.

Malicious Code Attacks

Malicious code is typically written to mask its presence thus it is often difficult to detect. Self-replicating malicious code, such as viruses and worms, can replicate so rapidly that containment can become an especially difficult problem. Dealing with malicious code attacks requires special considerations.

Virus Incidents

Issue: A virus is a self-replicating code that operates and spreads by modifying executable files. Viruses are often user-initiated and would pose virtually no threat if every user always followed sound procedures. In general, users should not execute attachments without first scanning for infection. E-mail executables tend to carry infections virus coding.

TMCC Action: TMCC has anti-virus tools in place, including a virus scanner on each TMCC-managed computer that checks every file opened, as well as a network scanner. TMCC maintains known good copy of anti-virus software on multiple network servers, separated by network domains. TMCC will immediately discontinue using any computer infected by a virus. Turn off the infected computer and call the ITO Help Desk. Do not attempt to eradicate the virus and/or restore the system without guidance from the ITO Help Desk.

Macro Viruses

Issue: Macro viruses are a type of virus that utilizes an application's own macro programming language to distribute themselves (e.g., Microsoft Word or Excel).

TMCC Action: Because macro viruses infect document files rather than programs, TMCC has extended its virus protection to include the examination of all files using the latest commercial anti-virus application. Macros are disabled by default on Microsoft Office applications.

Worms

Issue: A worm is a self-replicating code that is self-contained, (i.e., capable of operating without modifying any software). Worms are best noticed by looking at system processes. If an unfamiliar process (usually with an unknown name) is running and consuming a large proportion of a system's processing capacity, the system may have been attacked using a worm. Worms also sometimes write unusual messages to users' displays to indicate their presence. Messages from unknown users that ask the user to copy an electronic mail message to a file may also propagate worms. Worms generally propagate themselves over networks and can spread very quickly.

TMCC Action: If any TMCC employee observes the symptoms of a worm, he or she must inform the ITO Help Desk immediately. Prompt killing of any rogue processes created by the worm code will minimize the potential for damage. If the worm is a network-based worm, i.e., uses a network to spread itself, TMCC will disconnect any workstations or client machines from the network.

Trojan Horses

Issue: Trojan horse programs are hostile programs masquerading as valid programs or utilities. Most malicious code is really a Trojan horse program in one way or another. Trojan horse programs are often designed to trick users into copying and executing them.

TMCC Action: If any TMCC employee observes the symptoms of a Trojan horse, he or she must inform the ITO Help Desk immediately. Prompt killing of any rogue processes created by the Trojan horse code will minimize the potential for damage. If the worm is a network-based Trojan horse, i.e., uses a network to spread itself, TMCC will disconnect any workstations or client machines from the network.

Cracker/Hacker Attacks: Crackers and hackers are users who attempt to obtain unauthorized access to remote systems. The principal distinction between these two types of intruders is that "crackers" intrude with the intent of attacking specific systems, or inserting, deleting, or modifying specific data; "hackers" intrude for the thrill. Hackers may cause damage, but it is as an afterthought, not premeditated. Most cracking attacks are automated and take only a few seconds, which makes identifying and responding to them more difficult. Crackers now generally use "cracking utilities," which usually differ from conventional malicious code attacks in that most cracking utilities do not disrupt systems or destroy code. Cracking utilities are programs sometimes planted in systems by attackers for a variety of purposes, such as elevating privileges, obtaining passwords, disguising the attacker's presence and so forth. They can be used from outside the system to gather information as

well as launch attacks against the target systems. Cracking utilities are typically "a means to an end," such as obtaining administrative-level access, modifying audit logs, etc.

Modem Dial-in

Issue: Modem dial-ins are a favorite way to crack or hack systems.

TMCC Action: All modem lines connected to computers or servers are to be set as dial-out or made available on stand-alone PCs only.

Suspected Cracker or Hacker Compromise

Issue: Indications that a cracker or hacker may have compromised a system include the following symptoms:

- a) Changes to directories and files;
- b) a displayed last time of login that was not the actual time of last login;
- c) finding that someone else is logged into an individual's account from another terminal; or
- d) inability to login to an account (often because someone has changed the password).

TMCC Action: If these or other suspicious symptoms are noticed, the ITO Help Desk should be notified immediately. Use the [Incident Report form](#). If an attacker is caught in the act of obtaining unauthorized access, TMCC follows procedures dependent on the nature of the attack.

1. If the attacker has obtained administrative-level access, is deleting or changing user files, or has access to a machine that contains sensitive data, the attack poses a serious threat. In this case, the CIRT locks the attacker out of this system by aborting the processes the attacker has created.
2. If the cracker does not obtain administrative-level access and does not appear to be damaging or disrupting a system, the CIRT may elect to allow the attacker to continue so as to collect the evidence necessary to catch and/or prosecute the attacker.

Cracker or Hacker Activity Eradication

Issue: Because crackers so frequently use cracking utilities, it is important to ensure that no cracking scripts remain on the system once the cracker's attack has ceased. Another critical component of responding to cracker/hacker attacks is handling evidence that is gathered. System log printouts, copies of malicious code discovered in systems, backup tapes, referring to chains of custody and entries recorded in logbooks may conceivably be used as evidence against perpetrators.

TMCC Action: If a system user finds evidence of such cracking artifacts, the CIRT will make copies of the artifacts and forward them to TMCC IT Management and the TMCC Police Department for further examination. The CIRT will work to restore any file permissions and configuration settings that the attacker may have changed to their normal value. Resolving cracker/hacker attacks is risky, unless one possesses the technical skills, programs, and equipment necessary, which is specifically why the CIRT has been established.

Technical Vulnerabilities

Issue: As opposed to an internal or external threat, a technical vulnerability is a “hole” or weakness in an information system or components (e.g., system security procedures, hardware design, and internal controls) that could be exploited to violate system security. Most of the currently known technical vulnerabilities in applications and operating systems have been discovered and development testing and user acceptance testing.

TMCC Action: If a user discovers a technical vulnerability that could be used to subvert system or network security, he or she should immediately document that vulnerability and forward it to the ITO Help Desk using the [Incident Report form](#). Do not send vulnerability reports over the network or share vulnerability information with anyone outside of official channels. This document should record the following information:

1. Describe the vulnerability;
2. Describe the circumstances under which the vulnerability was discovered;
3. Describe the specific impact of the weakness or design deficiency; and
4. Indicate whether or not the applicable vendor has been notified.

PROCEDURES FOR RESPONDING TO INCIDENTS

TMCC defines six stages of response when servicing a computer security incident: preparation, identification, containment, eradication, recovery, and follow-up. Knowing about each stage facilitates responding more methodically and efficiently, and helps key staff understand the process of responding so that they can deal with unexpected aspects of incidents they face. The following defines the six stages of response.

Preparation

TMCC considers being prepared to respond before an incident occurs to be one of the most critical facets of incident handling. This advance preparation avoids disorganized and confused response to incidents. TMCC's preparation also limits the potential for damage by ensuring that response plans are familiar to all staff, thus making coordination easier.

Baseline Protection

TMCC has installed baseline protection on all systems and networks. All computing components have a first-line level of defense to keep incidents from spreading quickly from system to system. TMCC servers have access controls set so that none except TMCC server administrators can write to system executables. TMCC system administrators maintain compliance with Microsoft and Carnegie Mellon University Computer Emergency Response Team (CERT) notices, bulletins, and incident and vulnerability notes to ensure that all appropriate defenses are in place before an incident occurs. TMCC has obtained potentially useful tools in advance to avoid potential damaging delays that can occur when starting to procure such tools after an incident has happened. Examples include virus detection and eradication tools. TMCC continually monitors its networks for intrusions.

Planning and Guidance

TMCC has established a CIRT. Assigned system administrators will be available during a critical incident involving one or more essential systems. TMCC has planned for emergency communications needs. Should an incident adversely affect regular communication channels, TMCC has prepared lists of personnel to be contacted during incidents, including home phone numbers, cell phones, and pager numbers. See the TMCC Disaster Recovery Plan document.

Training

Training provided to CIRT personnel focuses on how to respond to incidents. CIRT members will participate in periodic mock incidents in which written incident response procedures are followed for simulated incidents.

Identification

TMCC's approach to the Identification Stage involves a) validating the incident; b) if an incident has occurred, identify its nature; c) identifying and protecting the evidence; and d) logging and reporting the event or incident. When a staff member notices a suspicious anomaly in data, a system, or the network, he or she begins the TMCC incident identification process.

Determine the Symptoms

Determining whether or not an anomaly is symptomatic of an incident is difficult since most often apparent symptoms of a security incident are something else, (e.g., errors in system configuration, application bugs, hardware failures, user errors, etc.) Typical symptoms of computer security incidents include any or all of the following:

- a) A system alarm or similar indication from an intrusion detection tool;
- b) Suspicious entries in system or network accounting logs (e.g., a user obtains root access without going through the normal sequence);
- c) Log discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which no entries whatsoever appear);
- d) Unsuccessful logon attempts;
- e) Unexplained, new user accounts;
- f) Unexplained, new files or unfamiliar file names;
- g) Unexplained modifications to file lengths and/or dates, especially in system executable files;
- h) Unexplained attempts to write to system files or changes in system files;
- i) Unexplained modification or deletion of data;
- j) Denial/disruption of service or inability of one or more users to login to an account;
- k) System crashes;
- l) Poor system performance;
- m) Unauthorized operation of a program or sniffer device to capture network traffic;
- n) "Door knob rattling" (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts);
- o) Unusual time of usage (remember, more computer security incidents occur during non-working hours than any other time);
- p) An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user; and
- q) Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

Identify the Nature of the Incident

Although no single symptom conclusively shows that a computer security incident is taking place, observing one or more of these symptoms prompts the observer to investigate events more closely. System administrators who encounter one or more of these symptoms should work with TMCC IT Management and designated IT points of contact to determine exactly what has occurred. TMCC will validate security incidents on a case by case basis. If the incident involves criminal activity or possible

criminal activity, TMCC IT Management will make a determination and, based on the outcome, will notify the TMCC Police Department.

Identify the Evidence

In order to protect the evidence, number, date and sign notes and printouts. Seal disks with the original, unaltered, complete logs in a safe or copy the entire log to an alternate location and secure appropriately. When turning over evidence to TMCC IT Management, ensure every item is signed for and detailed, factoring in the chain of command.

Protecting the Evidence

The chain of custody for all evidence must be preserved. Documentation will be provided that indicates the sequence of locations where the evidence has been stored. Dates and times must be specified and there must not be any lapses in time or date. The hand-off of evidence must be documented as well. The integrity of this information must be checked and provable in the anticipation that it may be challenged. This can be done by preserving the evidence on tamper-resistant media (e.g., CD-R), or generating cryptographic hash or checksum. TMCC obtains a full backup of the system in which suspicious events have been observed as soon as a computer security-related incident has been declared. Since perpetrators of computer crimes are becoming increasingly proficient in quickly destroying evidence of their illegal activity, be aware that, unless evidence is immediately captured by making a full backup, this evidence may be destroyed before it can be examined. This backup will provide a basis for comparison later to determine if any additional unauthorized activity has occurred.

Report the Events

If a computer-based incident is detected, it must be reported immediately to the CSO. In particular, each system owner must know how and when to contact the CSO. The [Incident Report form](#) attached to this guide should be used to gather information and report on the suspected incident. TMCC IT Management has the responsibility to report incident information to the college's senior leadership in a timely fashion. In addition, if there is evidence of criminal activity, the TMCC IT Management will notify the TMCC Police Department. CAUTION: No TMCC staff member, except the designated TMCC spokesperson (and the FBI, if involved) has authority to discuss any security incident with any person outside TMCC. The TMCC system and network audit logs provide sufficient information to facilitate deciding whether or not unauthorized activity has occurred. As soon as the TMCC IT Management and the respective system owners decide that a serious computer security incident has occurred that has wider ramifications, they will notify the TMCC Police Department and PIO.

Containment

TMCC's immediate objective for the containment stage is to limit the scope and magnitude of an incident as quickly as possible, rather than to allow the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator. The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. The TMCC IT Management and system owner will work within appropriate investigative organization(s) to determine if sensitive data should be left on the system or copied to media and taken off-line. Similarly, a

decision may be made to move critical computing services to another system on another network where there is considerably less chance of interruption. A decision on the operational status of the compromised system itself will be made. Whether this system be a) shut down entirely, b) disconnected from the network, or c) be allowed to continue to run in its normal operational status (so that any activity on the system can be monitored) will depend on the risk to assets threatened by the incident. In the case of a simple virus incident, the TMCC CIRT will move quickly to eradicate any viruses without shutting the infected system down. If the system is highly sensitive or information and/or critical programs may be at risk, TMCC will generally shut down the system down (or at least temporarily isolate it from the network). If there is a reasonable chance that letting a system continue to run as normal without risking serious damage, disruption, or compromise of data can identify a perpetrator, then TMCC may continue operations under close monitoring.

Maintain a Low Profile

If a network-based attack is detected, TMCC must be careful not to tip off the intruder. Avoid looking for the attacker with obvious methods - if hackers detect an attempt to locate them they may delete systems. Maintain standard procedures – continue to monitor for intrusions.

Avoid Potentially Compromised Code

It is not advisable to log in as root or administrator and then start typing commands to a system suspected of being compromised. For example, avoid using ftp to download tools from another site. If possible, record the fingerprint of critical binaries for the organization's core operation systems.

Back up the System

Back up the affected system to a new unused media. Do a backup as soon as there are indications that a security incident has occurred. Making a full backup immediately captures evidence that may be destroyed before having a chance to look at it. Make two backups; one to keep sealed as evidence and one to use as a source of additional backups.

Change Passwords

Immediately change the passwords on all affected systems. Passwords should be changed on compromised systems and on all systems that regularly interact with the compromised systems and notify all affected staff of the password change. If a sniffer device is detected or suspected, passwords may have been compromised on all systems on the LAN. It is important that users change to a unique password that is not being used on any other computer system.

Eradication

The next priority, after containing the damage from a computer security incident, is to remove the cause of the incident. In the case of a virus incident, TMCC will remove the virus from all systems and media (e.g., floppy disks, backup media) by using one or more proven commercial virus eradication applications. TMCC recognizes that many intrusions leave benign or malignant artifacts that can be

hard to locate. Therefore, TMCC will concentrate on the eradication of a) malignant artifacts (e.g., Trojan horses) and b) benign artifacts, only if they present a serious enough risk to justify the cost.

Determine the Cause and Symptoms

Use information gathered during the containment phase and collect additional information. If a single attack method cannot be determined list and rank the possibilities.

Improve Defenses

Implement appropriate protection techniques such as firewalls and/or router filters, moving the system to a new name/IP address, or in extreme cases, porting the machine's functions to a more secure operating system.

Perform Vulnerability Analysis

Use vulnerability analysis tools to scan for vulnerable systems that are connected to affected systems.

Recovery

TMCC defines recovery as restoring a system to its normal mission status.

Determine the Course of Action

In the case of relatively simple incidents (such as attempted but unsuccessful intrusions into systems), recovery requires only assurance that the incident did not adversely affect the FCC's computer or data resources. In the case of complex incidents, such as malicious code planted by insiders, recovery may require a complete restoration operation from backup tapes or full implementation of the FCC's disaster recovery plans.

Monitor and Validate System

First, determine the integrity of the backup itself by attempting to read its data. Once the system has been restored from backup, verify that the operation was successful and that system is back to its normal operating condition. Second, run the system through its normal tasks monitoring it closely by a combination of network loggers and system log files. Monitor the system closely for potential "back doors" that may have escaped detection.

Follow-up

TMCC realizes that devoting further resources to an incident after the Recovery Stage is not always cost effective. However, TMCC realizes that following up on an incident after the Recovery Stage helps to improve incident handling procedures.

Document Response Quality to Incident

- a) Obtain answers to the following questions to assess how well the agency responded to the incident:
- b) Was there sufficient preparation for the incident?
- c) Did detection occur promptly or, if not, why not?
- d) Could additional tools have helped the detection and eradication process?
- e) Was the incident sufficiently contained?
- f) Was communication adequate, or could it have been better?
- g) What practical difficulties were encountered

Document Incident Costs

Work internally to determine the staff time required to address with the incident (including time necessary to restore system). This leads to the following cost analyses:

- a) How much is the associated monetary cost?
- b) How much did the incident disrupt ongoing operations?
- c) Was any data irrecoverably lost, and, if so, what was the value of the data?
- d) Was any hardware damaged, and, if so, what was the cost? Deriving a financial cost associated with an incident can help in prosecuting, as well as serve as a basis to justify future budget requests for security efforts.

Preparing a Report

Depending on the type of incident, the FCC will prepare a report, including "lessons learned" and cost analyses described above. Those portions of the report that can be used to further the FCC's staff awareness (without endangering the FCC's security mechanisms) will be appropriately distributed and/or used in training.

Revising Policies and Procedures

TMCC realizes that developing effective computer security policies and procedures often requires revising those efforts in light of experience. Therefore, "lessons learned" from each incident are used to review TMCC's computer security measures.

Notification

The TMCC system displays a warning banner visible to all users who attempt to login to the system. The warning banner advises users that any unauthorized or access is prohibited and that the user accepts the rights and responsibilities in the TMCC Telecommunications Use Policy and the NSHE Computing Resources Policy. The login banner also that examination of information stored or accessed on the system may occur if authorized by the appropriate authorities.

Conclusion

These guidelines stress two fundamental principles related to incident response.

- a) The first principle is the importance of following well-defined and systematic procedures for responding to computer security-related incidents. The six stages of the TMCC's incident response procedures (preparation, detection, containment, eradication, recovery, and follow-up) provide a sound basis for securing the FCC's computer resources. They also serve as a foundation for developing custom procedures tailored to specific operational environments. The only effective way to respond to incidents is to use a structured methodology.
- b) The second principle is that unless conducted systematically, incident response efforts are of little value. Coordination of effort is a critical facet of incident response. TMCC staff members can significantly reduce the staff hours needed to respond to incidents if properly coordinated.

GLOSSARY

- a) **Anomaly:** An unusual or atypical event (in a system or network).
- b) **Attack Scanner:** A tool used to remotely connect to systems and determine security vulnerabilities that have not been fixed in those systems.
- c) **Cracker:** A person who obtains or attempts to obtain unauthorized access to computer resources for specific, premeditated crimes (see also Hacker)
- d) **Checksum:** Value computed, via some parity or hashing algorithm, on information requiring protection against error or manipulation.
- e) **Code:** System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.
- f) **Cracking utilities:** Programs planted in systems by attackers for a variety of purposes such as elevating privileges, obtaining passwords, disguising the attacker's presence.
- g) **Cryptographic:** A checksum that is generated using a checksum cryptographic means. It is used to detect accidental or deliberate modification of data.
- h) **Disruption of Service:** Disruption of service occurs when an intruder uses malicious code to disrupt computer services, including erasing a critical program, "mail spamming" i.e., flooding a user account with electronic mail, or altering system functionality by installing a Trojan horse program.
- i) **Encryption:** Using encryption renders information unintelligible in a manner that allows the information to be decrypted into its original form - the process of transforming plain text into cipher text.
- j) **Espionage:** Espionage is stealing information to subvert the interests of the FCC, the Federal government, or gaining access to a competitor's data to subvert contract procurement regulations.
- k) **Event:** Any observable occurrence in a computer system or network, e.g., the system boot sequence, port scan, a system crash, or packet flooding within a network. Events sometimes provide an indication that an incident is occurring, although not necessarily.
- l) **Firewall:** Used to control access to or from a protected network. Enforces a network access policy by forcing connections to pass through this system, where they can be examined and evaluated. The system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnets.
- m) **Hacker:** A person who obtains or attempts to obtain unauthorized access to computer for reasons.
- n) **Hoax:** A hoax occurs when false stories, fictitious incidents or vulnerabilities are spread (e.g., virus warnings that do not exist).
- o) **Incident:** An incident is defined as any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include penetration of a computer

system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software. Includes both deliberate attacks and accidental violations, but, for the purposes of these guidelines, the term "incident" does not encompass such events as natural disasters or failures of basic services to the general community (e.g., power outages, loss of telephone service, etc.) unless caused by deliberate act.

p) **Integrity:**

1. A sub-goal of computer security which pertains to ensuring that data continues to be a proper representation of information, and that information processing resources continue to perform correct processing operations.
2. A sub-goal of computer security, which pertains to ensuring that information, retains its original level of accuracy. Data integrity is that attribute of data relating to the preservation of:
 - a. its meaning and completeness,
 - b. the consistency of its representation(s), and
 - c. correspondence to what it represents.

q) **Intrusion:** Unauthorized access to a system or network.

r) **Malicious code attacks:** Include attacks by programs such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity.

s) **Misuse:** Misuse occurs when someone uses a computing system for other than official or authorized purposes.

t) **Sniffer:** A device or program that captures packets transmitted over a network.

u) **Social engineering:** "Conning" unsuspecting people into sharing information about computing systems (e.g., passwords) that should not be shared for the sake of security.

v) **Threat:** Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to, information or an information system.

w) **Trojan horse:** Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification or destruction of data.

x) **Unauthorized access:** Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to obtaining unauthorized access to files and directories and/or by obtaining "super-user" privileges. Unauthorized access also includes access to network data gained by planting an unauthorized "sniffer" program (or some such device) to capture all packets traversing the network at a particular point.

y) **UUOS:** UUOS occurs when an intruder gains unauthorized access to data by planting programs such as a Trojan horse. Other examples include: using the network file system (e.g., Novell) to mount the file system of a remote server machine, using the Virtual Memory System (VMS) file access listener to transfer files without authorization, or using the inter-domain access mechanisms to access files and directories in another organization's domain.

- z) **Virus:** Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.
- aa) **Vulnerability:** Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.
- bb) **Worm:** Independent program that replicates from machine to machine across network connections often clogging networks and computer systems as it spreads.

Originating Policy or Source: TMCC Telecommunications Use Policy; IT Standing Policy for Network and Operational Security

Responsible Office: Information Technology Operations and Information Technology Services

Updated: September 2008