Infrastructure & Sustainability (I&S)
Information Security Policy

Last Revised: November, 2021

1 PURPOSE

The purpose of this policy is to provide requirements and specific recommendations for the protection of I&S *information technology resources* and the information stored on those resources. Information security measures are intended to protect information assets and preserve the privacy of the Institute's employees, students, sponsors, suppliers, and other associated entities.

All *employees* of *I&S* are bound by this policy as well as other Institute policies as terms of their employment. All employees share responsibility for the security of the information in their directorates. If any conflicts arise between the I&S policy and the Institute Computer and Network Usage policy, this policy prevails.

> (**NOTE**: phrases which are shown in *italics* at their first occurrence in this document are defined in Section 9, Definitions.)

2 SCOPE

This policy applies to all directorates under the purview of I&S. It covers all I&S information technology resources and information that is stored digitally using information technology covering past, present and future activities of I&S. All creation, processing, storage, communication, distribution, and disposal of I&S information in digital form are covered by this policy.

3 POLICY

Digital information is considered a I&S corporate asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, destruction, or denial. Information security controls must be sufficient to ensure the *confidentiality*, *integrity*, *availability, accountability, and auditability* of important information (the five components of information security). For the purposes of this policy; data and information technology resources owned by a sponsor or client but is being used by I&S, shall be considered "owned by I&S." Under Georgia Law some information may be required to be disclosed under the Open Records Act. If you are contacted to disclose information, please refer the request to GT Legal, notify your manager, and ensure that GT Legal is notified of the request.

Each I&S directorate is required to determine the proper levels of protection for their information technology resources and information and to implement the necessary safeguards. All I&S employees are expected to cooperate in carrying out the provisions of this policy.

Information security controls must be applied in a manner consistent with the value of the information. More critical or sensitive information and information technology resources will require more stringent controls. This policy does NOT supersede the procedures for data categorization or access controls specified in the Institute's *Data Access Policy* http://policylibrary.gatech.edu/data-access. Department of Defense (DoD) requirements for handling their classified information are detailed in a separate document.

4 SECURITY INCIDENT REPORTING

All actual or suspected instances of information technology abuse or information asset theft, as well as potential threats (hacker activity, computer viruses/worms, natural disasters, evidence of forced entry, etc.), **must** be reported at once to *departmental computer support* or the Director/Manager in the affected directorate. Based on the seriousness of the situation, departmental computer support or the director/manager may report the incident to GT Information Security.

The departmental computer support or the directorate Director/Manager will report serious, or potentially serious, breaches of information security to the appropriate person(s) in GT Information Security, who is responsible for all coordination with local, State and Federal law enforcement authorities. The Institute's Computer and Network Usage Policy GT Computer and Network Usage Policy gives additional details of the reporting procedures and guidance for assessing the extent and seriousness of an information technology security breach.

5 PRACTICES TO IMPLEMENT THIS POLICY

The specific procedures and practices to implement this policy will vary by I&S directorate and with the importance of the information and resources being protected. Responsibilities for complying with these practices are listed in Section 6, and some recommended procedures are outlined in Section 8. Each directorate shall:

A. Limit access to information and communication systems solely to individuals authorized by management.

B. Protect all information technology resources (e.g. computers, communications, software, data) from theft, tampering, misuse, malicious software (e.g. malware, *viruses, worms, Trojan Horses*), destruction, and loss.

C. Managers must facilitate access to policies; however, employees are bound by this policy and other Institute policies as terms of their employment. http://policylibrary.gatech.edu/information-technology/cyber-security-policy

D. Ensure individual and organizational accountability for the use and protection of information technology systems through the use of unique identifiers and authentication methods (e.g. userID/password, *digital certificates*, or *biometrics*).

E. Prohibit the sharing or unauthorized disclosure of passwords or other confidential access information (e.g. access phone numbers, codes, network information).

F. Require prompt notification per section 8.1.4 of changes in status (e.g. transfers, terminations, retirements) of employees, sponsors, or other users of I&S IT resources.

G. Control access to information based on criteria defined by the assigned *data steward*(s) as established in the Data Access Policy. (NOTE: this requires that all significant collections of information in I&S have a defined data steward).

H. Apply appropriate controls to ensure only authorized use of software and hardware that is designed for bypassing or breaking through information security measures and procedures. Ensure appropriate audit procedures are established to monitor for inappropriate use software and hardware that is capable of bypassing or breaking through information security measures and procedures.

I. As necessary, produce, review, follow up and retain audit trails of IT-security-relevant information for all systems that process and store Category 2 or Category 3 data as established in the Data Access Policy.

J. Regularly perform self-assessments and/or audits to detect security vulnerabilities and non-compliance with I&S Information Security Policy and defined procedures.

K. Apply *cryptography* as appropriate to protect critical information which must be transmitted or stored on communication circuits and systems which are less secure than the usual I&S network and systems – for example, sent over the Internet, sent over wireless, or stored on laptops while traveling.

L. Ensure that IT resources are procured with the capability to use security features to help implement this policy, such as UserID/passwords, system integrity protection, auditability.

M. Maintain continued availability of business-critical IT resources and information through plans and procedures, such as for backup, recovery, redundancy, *disaster planning*, etc.

N. Define and apply information retention procedures that satisfy external and internal requirements. While defining and applying procedures to dispose of information that is no longer needed.

6 RESPONSIBILITIES

6.1 Employees (as defined in section 9)

Each I&S employee is responsible for complying with the policies and procedures relating to information technology security and for fully cooperating with the IT staff within their directorate to protect the IT resources of I&S and the Institute.

For purposes of this policy each employee must become familiar and comply with the Institute's Computer and Network Usage Policy located online: http://www.security.gatech.edu/policy/usage.html

I&S computer and communications systems must be used for business purposes only. Incidental personal use is permissible if the use (a) does not consume more that a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with worker productivity, (c) does not preempt any business activity or violate any law, and (d) does not increase the security risk. Examples of permissible incidental use are – the occasional use of electronic mail (email) or web access for other than official purposes.

Activities such as loading unauthorized software on I&S systems, using I&S systems to access pornographic materials and unauthorized downloading of copyrighted material (e.g. music or movies), places the Institute at risk and are not permitted. Conduct in violation of this policy may result in sanction as provided in Section 7 of the Computer and Network Usage Policy. Report all actual or suspected instances of security or policy violations in accordance with Section 4 of this policy.

All computer hardware and software acquired for or on behalf of I&S or developed by I&S employees is I&S property.

Employees who are leaving the employ of I&S for any reason shall immediately return the original and all copies of all Department-owned software, computer materials, or computer equipment that is either in their possession or otherwise directly or indirectly under their control.

6.2 I&S Senior Management

Senior management of I&S is responsible for:

A. Promulgating and enforcing the policies, standards, procedures, and guidelines for the protection of IT resources and information.

B. Appointing a Computer Support Representative, and providing appropriate funding, training, and resources to those people for information security-related tasks.

C. Applying sanctions consistent with Human Resources policies to individuals and department heads that break provisions of this policy, either willfully, accidentally, or through ignorance.

D. Designating Data Stewards for each significant collection of business information, who in turn are responsible for determining the value of their information and implementing appropriate security measures as specified in the Data Access Policy

E. Furnishing funding and other resources or limiting and eliminating services to ensure continued compliance with this policy.

F. Sponsoring internal awareness and training programs to familiarize employees with the security policy, procedures and recommended practices.

G. Defining guidelines and intervals for each directorate to carry out periodic self-assessments to evaluate compliance with this policy and to identify potential risks to IT resources and information.

H. Document the unit's service models for both the services the unit offers to the Internet at-large, to the Campus networked community and internally to the unit; and the services the unit requires access to, from the Internet at-large (e.g. web access) and from the Campus network (e.g. email). This document must be prepared by Unit Directors and approved by the appropriate VP.

7 CHANGES TO THIS POLICY

This policy may be temporarily changed by directive of the Vice President of I&S for any reason, but typically in response to new types of threats or risks. Notice of the change in the policy must be distributed to all I&S directorates and departmental computer support. The changes may not be extended over six (6) months without being submitted and approved formally through the GT Information Security policy change process.

8 RECOMMENDED PRACTICES AND PROCEDURES

Within this Section, the phrases "must" and "recommended" have specific meanings where highlighted in **boldface**. If a I&S directorate correctly adheres to the guidelines given as "**must**", then it can be considered as meeting the requirements for this policy. If they also adhere to the guidelines given as "**recommended**", then they can be considered to be meeting the "Level One" (minimum) requirements for information technology security generally promoted by many experts (reference: Fundamentals of Effective Network Security, SANS Institute).

Recommendations for maintaining good security of information and IT resources can be divided into two broad areas: (1) People/Funding and (2) System/Network Management.

8.1 People/Funding

8.1.1 Departmental Computer Support

I&S ***must*** have at least one non-student person who is designated as "departmental computer support". The support person(s) must have a combination of appropriate skill levels to correctly manage all of the different computers, operating systems, and application software in use within the unit. The unit may choose whether to "purchase" support from an outside individual, I&S unit or other organization, or to employ one or more people within the unit to provide the support. It is ***recommended*** that at least one person be funded full-time for each fifty (50) computers being supported (more staff may be required if the unit does not actively minimize diversity – see Section 8.2.1.). Students may be employed to assist in this effort, as long as at least one permanent employee with a technical background provides supervision and provisions are made for continuous coverage of the student position(s).

The person(s) designated as departmental computer support for the unit ***must*** have management support, funding, training, materials, and other resources as necessary to correctly manage the computers, printers, and other IT resources they support. NOTE that assigning insufficient resources in this effort creates risks of IT security compromises.

8.1.2 Cyber Security

ALL I&S staff are responsible for protecting the GT resources (data, systems and equipment) which they access and use. All staff must follow the ***Security Procedures and Standards*** published by Georgia Tech Cyber Security including the Georgia Tech ***Protected Data Practices***. For a review of the Cyber Security policy, follow this link.

8.1.3 General I&S Staff

The responsibilities for IT security of each person who uses any I&S IT resource ***must*** be communicated to them at, or immediately after, hiring. This should become part of I&S induction procedure for all new hires. This should be supplemented with periodic additional training. The following topics ***must*** include:

- Password policy and how to choose good passwords.
- Prohibition of unmanaged modems/remote access communication lines.
- Comply with section 8.2.3 remote access guidelines.
- Defense against "*social engineering*" tactics to gain unauthorized access to systems.
- Location and identity of their computer support staff, the Director/Manager for their directorate, and the GT Information Security office.
- How to get access to the GT Computer and Network Usage Policy.
- Recommendations about physical security (e.g., lock up your office when leaving, protect information on a portable when traveling, protect systems from theft or damage).
- Other topics as deemed necessary or timely by the directorate Director/Manager or the newly hired person's departmental computer support.
- Review the information security tutorial located online: (http://www.security.gatech.edu/tutorial.html)

8.1.4 Employee Termination and Clearance

I&S ***must*** establish a procedure for confirming that directorate directors and their managers ensure that all access rights to I&S resources (information or physical) are revoked immediately upon any significant shift in job responsibilities (e.g. transfer between directorates within I&S, transfers outside I&S, retirement, termination, or reclassification). This policy recognizes that exceptions exist to this policy (e.g. retirees retain their e-mail address for mail forwarding as they deem appropriate).

8.2 System/Network Management

Every computer system used by I&S ***must*** be managed by a member of the departmental computer support for that business directorate. I&S and project managers should account for this need when planning budgets for projects and for internal computer support. "Management" authority of the system for security includes at least:

- Physical access to the system at all times;
- Ability to use the controlling account for the computer (e.g., "root" or "Administrator");
- Authority to change the system configuration, reboot the system, and/or disconnect/connect the system to the GIT network as needed;
- Authority to manage and view the system logs, security logs, user access logs, etc.
- Installation or modification of system software or hardware

Networking technologies may be added to the GIT network **only** with the approval of the OIT authorized directorate or department.

In keeping with section 6.2, item h, all additions, modifications, or removal of network services (e.g. web servers, DNS servers, file servers) will be documented in a common point and receive appropriate senior level management approval. All new network services or major modifications to existing network services extending outside I&S firewall ***must*** be certified via the service certification process.

Provisions must be made to allow emergency access to systems when the system administrator may not be available.

8.2.1 Minimize Technology Diversity:

If there exists in the directorate a great variety of computer equipment, operating systems, and applications, then it becomes very difficult and expensive for the computer support staff to understand, keep updated and effectively utilize all the different IT-security measures. Therefore, to the greatest extent possible, the number of ***different*** brands, models, sizes, and versions of equipment, software, & operating systems should be minimized.

To ensure this requirement is met, all purchasing of Department computer hardware and software shall be centralized with the I&S Information Technology (IT) directorate to ensure that all hardware and software conforms to Department standards, will integrate into the current computing environment, and is purchased at the best possible price. All requests for computer hardware or software must be sent to the IT directorate, which will determine the hardware or software that best accommodates the desired request. Once the total cost is known, the requestor will follow whatever

purchase approval processes have been established within the requestor's work unit, including any Purchase Card (P-Card) approval processes.

8.2.2 Change Management, Patches and Updates:

Departmental computer support ***must***:

A. Provide a documented and standardized process for change requests, approval, and testing

B. Electronically log changes in a spreadsheet or OIT provided change management system, thus to assure the completeness of the changes made into the target system(s).

C. Monitor published information from the appropriate Georgia Tech mailing list and, where appropriate, various security sources and vendors related to security risks on the computer systems they support.

D. Download or purchase the appropriate vendor-recommended patches, updates, fixes, scripts, and so forth that will mitigate the reported security risks.

E. Apply the patch, script, update, etc. either on a regular basis or immediately, depending on the seriousness of the security threat, the category of the protected information, and the appropriate vendors' inputs.

8.2.3 Manage Access Control Information

Each IT system ***must*** have access control measures in place, such as unique user IDs and passwords for login to the computer and some level of physical security (e.g., all equipment behind locked doors during non-work hours). User IDs ***must*** be unique to the user and not shared, and that password formats and contents follow a strong password policy:

- At least 8 characters (at least 11 characters where better security needed)
- Not a "dictionary" word or a common proper name
- At least one number or special character included
- Passwords changed on a regular basis (at least every 120 days)
- Passwords are not written down anywhere that is readily available during a casual search of a person's work area

It is ***recommended*** that, when necessary and possible, directorate management direct the departmental computer support to force compliance with the userID/password policy through features of the operating system(s) and with regular scans to find passwords that can be easily decoded. Additionally, a quarterly scan and review of users, roles and access permissions to be conducted by senior IT administrators, to ensure accounts/roles are current.

All directorates within I&S ***must*** use a common "remote users" communications facility, to be professionally managed and supported, to meet the needs of I&S off-site users while maintaining good security. Where a directorate of I&S determines

that it must have an independent remote user communications facility, security measures equivalent in strength (to the common remote users' communication facility) ***must*** be applied to this access path. Such security may include stronger enforcement of the userID/password policy, possible restrictions on hours of availability, possible restrictions on permitted userIDs, and other measures as appropriate and feasible. An outsider with malicious intent who gains access to the network via this path can potentially access any node in Georgia Tech.

Additionally, user access to be granted, deactivated, updated or terminated via a documented and reviewable procedure, such as an online form and will follow USG user access controls guidelines (5.12.1). https://tinyurl.com/2mfzp3u6

Participation in a remote access program may not be possible for every employee. An employee's eligibility to remotely access the Department's computer network will be determined by his or her supervisor. Remote access is meant to be an alternative method of meeting Department needs. The Department may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

No unmanaged dial-in lines with modems are permitted within I&S. Each of these is potentially an open security hole for I&S and the entire GT campus.

8.2.4 Logon Banners

All computers and remote users communications facilities within I&S, if capable, ***must*** be configured to display a *pre-logon banner*, which explicitly states that unauthorized access is prohibited; the banner may optionally include a reference to the GT Computer and Network Usage Policy. GT Information Security shall determine the exact wording of the pre-logon banner, in consultation with GT Legal.

8.2.5 Connection and Port Control

All computers with a modern operating system are vulnerable to well-directed attempts to gain unauthorized access or to overload the computer in order to deny access to legitimate users. Success in these attempts often allows the attackers access to many other systems, both in I&S, the GT network, and even throughout the entire Internet community. The best defense against these intrusions or denial-of-service attacks is for a skilled and knowledgeable system administrator to keep the operating system and software up-to-date with patches and updates that defend against known security problems (See Section 8.2.2 above)

All I&S directorates ***must*** take some measures to deny intrusion, probing, and denial-of-service attempts through the network, such as:

- Network connection/attack monitoring/anti-virus software; (http://software.oit.gatech.edu)
- An effective and well-supported network-based firewall node(s) based upon the Service Model spreadsheet and unit-level policy.
- At a minimum, a proactive system of applying the correct patches and updates to every supported computer system immediately once a security problem has been identified and published.

Appropriate measures to apply will vary with the operating system and the degree of threat. It is ***recommended*** that the effectiveness of the steps taken be tested on a regular basis with a network-based vulnerability scanner (e.g. FireEye, Qualys, Nessus), and necessary improvements made in a timely manner. Consultation with the Computer Support Representative and GT Information Security is critical in this effort.

8.2.6 Virus/Worm Control

Due to the increasingly severe threat from viruses and worms, and the speed at which they spread, directorates of I&S ***must*** put in place measures to control them. Typical measures include installing and keeping updated a commercial software package (e.g., McAfee Anti-Virus) on every computer connected to the network or which receives email or runs software from the GIT network. To help with this effort, OIT maintains a site-license for anti-virus software. The same type of proactive efforts as outlined in Section 8.2.2., above, are recommended in order for the computer support staff to keep the anti-virus software updated and capable of stopping viruses and worms before they do damage to systems.
(https://software.oit.gatech.edu)

Departmental computer support are the only employees authorized to send Department-wide computer virus alerts. Other employees who suspect their Department-owned computer is infected with a virus should contact departmental computer support. Members of the computer support team will validate the virus threat and ensure necessary precautions are taken, which may include sending a Department-wide virus alert.

8.2.7 Ancillary Systems Backup and Disaster Recovery

In order to maintain the *availability* component of information security, each support directorate of I&S ***must*** have a system implemented, maintained, managed, and tested that duplicates and preserves business-critical data. Depending on the importance of the information, some duplicate copies of the data may be kept “off-site”, or preserved against physical damage from fire, water, theft, erasure, etc. A “system” includes hardware, software, and trained staff with known procedures to follow.

It is ***recommended*** that these systems be regularly tested to ensure that the data can be recovered, starting from the assumption that the original data and the hardware on which it was stored is not available. Review and testing of these disaster recovery procedures must be done, at a minimum, every 24 months. At least one test is required when a system is implemented, also when major components of the system change.

It is ***recommended*** that I&S follow the IT disaster recovery plan created using GT Ready (https://gatech.kuali.co/ready), and that all departmental computer support and in-directorate managers be familiar with this plan and in agreement about how it should be executed. The procedure for briefing a newly hired manager or departmental computer support person should include an overview of backup procedures and the disaster recovery plan, and a copy for their files.

8.2.8 Physical Security

Maintaining information security requires some measures of physical security as well; ***recommended*** measures include:

- Major file and computing servers should be placed in *limited-access room(s)*. At least one full copy of a system backup should be stored away from the system or off-site.

- Network equipment and cable patch points should be placed in limited-access rooms, with only network-knowledgeable, authorized support staff permitted to work in those rooms.
- Individual computers (generally for one person's use) should be in rooms that are locked during non-work hours.
- Only departmental computer support should add or remove software or parts from a computer.

Computers physically accessible to more than one user should have password-protected screen savers enabled. Computers actively used by more than one person should be setup to maintain user accountability and auditability.

8.2.9 Accountability and Auditing

On systems which can have effective access controls (e.g. Windows 10, UNIX), a login process should always be required which can potentially capture the userID of the person logging on and the time at which they logged on and off. "Autologin" procedures are discouraged. On systems where the security need is higher, the capture of this information should be enabled, and the audit log scanned on a regular basis. For remote user communication facilities, this information should ***always*** be captured and saved, and backed up for a defined period of time, and if possible, regularly analyzed for evidence of attempted security breaches.

On systems which contain more critical amounts or types of data, such as servers of any type, system auditing of major events ***must*** be enabled, and a regular scan of the audit files ***must*** be performed – manually or automatically - to detect unusual events. It is ***recommended*** that major system files be *fingerprinted* and the records stored on a secure system or media, for use in detecting intrusions and compromises (put procedures in place such that each upgrade or patch of the system causes another fingerprint to be taken and stored).

8.2.10 Data Governance and Management

The effective and responsible use of information requires that data must be secure and accessible for use by trained and authorized personnel as outlined in the *Data Governance and Management policy*. This policy is in compliance with the USG business procedures manual.

8.2.11 Bring Your Own Device (BYOD) Standard

This standard applies to any I&S staff that uses personal IT equipment to access GT provided resources. Access to these resources is a privilege, not a right and does not guarantee ongoing access to these resources. For additional information on this USG standard, follow this link.

9 DEFINITIONS

Availability – The percentage of time (compared to 100%) during which you can retrieve information when needed. Information can be unavailable due to destruction/erasure, system or network not working, or needed retrieval resources being overused.

Biometrics – The use of hardware and software to authenticate a person by measuring characteristics of their body, such as fingerprints, facial size and feature arrangement, handwriting style and speed, etc.

Confidentiality – The amount of confidence that information has not been disclosed to any person not authorized to view, copy, or distribute that specific information.

Cryptography – Using programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key – usually a user-selected key.

Data Access Policy – The Institution policy establish governing the categorization of data and the appropriate access controls required based on that categorization. http://policylibrary.gatech.edu/data-access

Data Steward – While the final definition of this term rests with the Data Access Policy, three roles are spelled out in the policy. Chief Data Stewards are responsible for establishing Data Steward roles and clear defining responsibilities. Data Stewards are responsible maintaining appropriate access controls to and auditing of Data under their purview. Additionally, Data Stewards are responsible for establishing Data Coordinators. These positions are responsible for assuring the quality and condition of the data.

Denial-of-Service Attack – A form of damage performed by malicious code, where the intent is to overload the target computer(s) or network resources such that legitimate users cannot effectively use the resources.

Department Computer Support – The person(s) in each department or from an external entity but funded by the directorate, designated to procure, install, inventory, troubleshoot, and otherwise manage the information technology resources of that lab or support group.

Digital Certificates – A high-security form of authentication - the exchange of short, encrypted files by the programs that are communicating, which serve to authenticate the client and server processes to each other. There is an entire system of organizations and protocols that work together to create, authenticate, revoke, and use digital certificates. The user of a computer typically allows the program(s) to use digital certificates by logging in to the system or program with a user ID/password.

Disaster Planning – Creating, implementing, and testing plans and procedures for the continuation of essential business operations even after a disaster, such as an earthquake, hurricane, flood, extended power outage, terrorist incident, etc. Usually involves duplicated computing facilities, communications facilities, vendor agreements, employee procedures, etc.

Employees – Faculty, classified employees (as defined by the employee handbook), and student employees

I&S - The systems and personnel under the purview of the Vice President of I&S

Fingerprinting (of files) – Creating a mathematical summary of the file which is usually sufficient to detect any change to the file, but can be stored compactly (e.g. a hash or CRC of the entire file).

Information Technology Resources – Computers, storage peripherals, network equipment and wiring, network-attached printers and fax machines.

Integrity – The amount of confidence that the information has not been modified in an unauthorized or incorrect way.

Limited-access room – A room that only a limited number of people possess keys to enter the room and authority to manage the IT equipment within the room.

Pre-logon banner – A message that is shown to the person attempting to login to a computer or communications facility BEFORE they are prompted to enter any authentication (user ID/password, biometrics, etc).

Read Access Group – The group of people allowed to read a given set of information. At least four (4) groups are defined for this Policy: OWNER ONLY, GTRI ONLY, GIT ONLY, and PUBLIC.

Social Engineering – The collective term for many tactics used by people attempting to break security measures of an organization by working with staff members' desire to be helpful or their ignorance of proper security measures. An example would be an intruder posing on the phone as a new system administrator or auditor, who asks for your user ID/password "to check security on a system."

Trojan Horse (program) – A program which consists of malicious code, but which is promoted as or appears to be a useful program, in order to trick an unsuspecting person into executing the program.

Virus – A fragment of code that is hidden within an executable program or system boot block, that when run by an unsuspecting user, replicates itself into other locations, and may optionally do damage to the information stored on the executing system.

Worm – A self-contained program that runs itself on a system, which replicates to other systems and may optionally do damage to the information stored on the executing system, or perform denial-of-service activities on the network(s) that the systems are attached into.

10 APPROVAL

_____

VP-I&S

_____

Effective Date