IT Security Plan

INTRODUCTION (Purpose and Intent)

The USF IT Security Plan defines the information security standards and procedures for ensuring the confidentiality, integrity, and availability of all information systems and resources under the control of USF Information Technology. Included are:

- Definitions and descriptions of terms and acronyms used in the USF IT Security Plan and related documentation
- The roles and responsibilities of individuals and groups within the USF System
- Descriptions of or links to descriptions of standards and procedures for:
  - Information system security plan and documentation
  - Security concerns in system management
  - Technology acquisition
  - System access, use, and resource security
  - System and data integrity
  - Data classification and restrictions
  - Risk management
  - Security incident response
  - Security awareness and training
  - Security audits

The USF IT Security Plan supplements the Official Security Policies, Standards, and Procedures that have been established for the USF System. This security plan is intended to comply with the regulations and policies set down by the State of Florida, the University of South Florida, the *Federal Information Security Management Act* (FISMA), and other state and federal regulations.

SCOPE

The standards and procedures set down in the USF IT Security Plan apply to all information systems and resources connecting to the USF System network.

DEFINITIONS

Accountability	The state in which an individual or group is answerable and held accountable for their or its activities.

Acquisition	In the context of this document, gaining possession, through purchase or lease, of assets and/or services related to information technology, such as computer hardware, software, or services.
Accreditation	In information system security, the formal authorization for system operation and an explicit acceptance of risk given by the accrediting (management) official. It is usually supported by a review of the system, including its management, operational, and technical controls.
Audit	In IT, an independent, unbiased examination of an information system to verify that it is in compliance with its own rules; the process of collecting and evaluating evidence of an organization's security practices and operations in order to ensure that an information system safeguards the organization's assets, maintains data integrity, and is operating effectively and efficiently to meet the organization's objectives.
Auditable event	A single action (either a command or system call) that affects the security of an information system.
Backup	The process of backing up (copying onto electronic storage media) data that may then be used to restore the data to its original form after the occurrence of a data loss event or data file corruption. Two backup types are referenced in this document o full – a complete backup of all data, whether or not changes have occurred o incremental – a backup of only those files that have changed or been added since the last full or incremental backup was performed
Corrective Maintenance	A form of system maintenance performed after a problem or failure is detected in an information system, with the goal of restoring operability or peak performance to the system.
Criticality	Degree of value.
Data Corruption	The result of errors in computer data that occur during electronic writing, reading, storage, transmission, or processing, that introduce unintended changes to the original data. Generally, when data corruption occurs, the file containing the data becomes inaccessible and/or unusable.
Data Integrity	The accuracy, completeness and consistency of data stored in an information system, free from either accidental or deliberate, but unauthorized insertion, modification or destruction of data in a database.
Disaster	In the context of information systems, 1) an emergency or other event resulting in the destruction, theft, or corruption of data; 2) an inability to access an information system and/or its data for longer than a reasonable

	period, the duration of which is determined by the criticality of the system resources and data; 3) extensive damage inflicted on an information system, the availability of which is necessary for the maintenance of confidentiality, integrity, and availability of data required for the operation of an organization.
Disaster Recovery	The process, policies, and procedures preparing for recovery or continuation of the technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery includes planning for resumption of operating system and application software, data, hardware, and communications (networking).
Distributed system	An information system composed of multiple autonomous computers that communicate through a computer system.
FISMA	The Federal Information Security Management Act of 2002, which recognizes and addresses the importance of information security to the economic and national security interests of the United States. FISMA sets down information security requirements that must be followed by federal agencies, as well as any other parties, agencies or organizations collaborating with such agencies, in an effort to maximize their effectiveness in safeguarding information systems and the data contained within information systems.
Hacking	Detecting weaknesses in a computer or computer network. Hacking tools are programs designed to assist with hacking; these programs are often malicious and may be used to detect and exploit vulnerabilities in operating systems and/or user accounts.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, which sets national privacy standards for the protection of certain types of health information to the extent such information is electronically transmitted by health plans, health care clearinghouses, and health care providers.
Information system	An integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, communications, and digital products, support, and services.
IT	Information Technology
IT resources	All USF system computing facilities, equipment, hardware, software, data, systems, networks and services that are used for the support of the teaching, research and administrative activities of the USF System
Maintenance window	The period of time designated in advance by a technical staff during which preventive maintenance that may cause disruption of service will be performed on an information system.

National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the U.S. Department of Commerce. The mission of the NIST is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life in the U.S.
Network/system topography	Describes the arrangement of systems on a computer system, defining how the computers, or nodes, within the system are arranged and connected to each other.
Non-technical controls	Management and operational controls such as security policies, operational procedures, and personnel, physical, and environmental security.
Preventive maintenance	A form of system maintenance conducted on a regular basis and intended to maintain and/or improve information system performance, avoid unplanned downtime, keep system software programs up-to-date, and prevent problems from occurring on an information system.
Protected data	Any data governed under federal or state regulatory or compliance requirements (such as FERPA or HIPAA), as well as data deemed critical to USF business and academic processes which, if compromised, may cause substantial harm and/or financial loss.
Residual risk	As it pertains to USF IT, any risk (vulnerability or exposure to loss or harm) that remains after mitigation of a risk or risks identified through the security risk assessment process.
Restricted data	Highly sensitive information intended for limited, specific use by individuals, workgroups, departments, or organizations with a legitimate "need to know." On USF System information systems, data stored digitally that requires restrictions to its access and dissemination, as defined by federal or state law, or by USF policies and standards.
Risk	The probability that a particular vulnerability or vulnerabilities in the USF information system will be intentionally or unintentionally exploited by a threat which may result in the loss of confidentiality, integrity, or availability, along with the potential impact such a loss of confidentiality, integrity, or availability would have on USF operations, assets, or individuals.
Risk analysis	The process of identifying the most probable threats to USF information systems, revealing how frequently particular undesired events occur, and of determining the criticality, causes, and consequences of these threats and/or events.
Risk assessment	The overall process of risk analysis and risk evaluation and a key component of risk management that involves identifying and evaluating

Risk evaluation	The process used to determine priorities for risk management by comparing the level of risk against predetermined standards, target risk levels, or other criteria.
Risk management	The overall process for identifying, controlling, and mitigating security risks to information systems. USF System IT risk management comprises risk assessment, risk analysis, and treatment of risk, and includes the selection, implementation, testing, and evaluation of security controls.
Risk mitigation	The systematic reduction in the degree of exposure to a risk and/or the probability of its occurrence.
Security	In IT, the preservation of confidentiality, integrity, and availability of an information system and/or the data that resides on it.
Security authorization	The official management decision made by a senior organizational official to authorize operation of an information system and to accept certain risks to organizational operations and assets, individuals, and other organizations based on the implementation of an agreed-upon set of security controls.
Security incident	Any computer or network-based activity that results (or may result) in misuse, damage, or loss of confidentiality, integrity or availability of an information system and/or the data that resides on it.
Sensitive data	Any data which, if compromised with respect to confidentiality, integrity, and/or availability, could have an adverse effect on the organization's interests, the conduct of its programs, or the privacy to which individuals are entitled.
Sensitivity	A measure of how freely data stored on an information system can be handled.
Software patch	An update that fixes bugs (errors, flaws, mistakes, failures, or faults), increases security or adds new features to a software program. A patch typically does not include substantial enough changes to warrant a new version or release of the entire program.
Software update	Modification to an existing version/release of a software program to develop or improve upon its features, function and/or performance without upgrading it to a new major version.
Software version upgrade	Replacement of a software program with a newer version of the same program in order to bring it up to date or to develop or improve upon its features, function and/or performance.

Storage area network	A dedicated system that provides access to consolidated, block level data storage; a system with the primary purpose of transferring data between computer systems and storage elements.
ST&E	Security Test and Evaluation
System development life cycle (SDLC)	A conceptual model used in project management that describes the phases involved in an information system development project. A typical information system life cycle includes these phases Initiation – the system is described in terms of its purpose, mission, and configuration. Development and Acquisition – the system is constructed according to documented procedures and requirements Implementation and Installation – the system is installed and integrated with other applications, usually on a network. Operational and Maintenance – the system is operating and maintained according to its mission requirements. Disposal – the system's life cycle is complete; it is deactivated and removed from the network and active use.
System integrity	The state or quality of an information system when its intended functions are performed in an unimpaired manner, free from either intentional or accidental, but unauthorized manipulation, changes or disruptions.
System maintenance	The adjustment or modification of an information system to correct faults, improve performance, adapt to change in requirements, or changes in the system environment.
System management	The administration/oversight of a distributed computer system, which may include development, configuration, maintenance, and security and contingency planning.
Technical controls	Safeguards that are incorporated into computer hardware, software, or firmware, such as access control mechanisms, identification and authentication mechanisms, encryption methods, and intrusion detection software.
Threat	Any circumstance or event that has the potential to intentionally or unintentionally exploit a particular vulnerability in the USF Health information system, resulting in a loss of confidentiality, integrity, or availability.
USF	University of South Florida
USF IT	USF Information Technology that provides support to USF Tampa campus

USF Unit	USF regional campus, College or Department that provides IT services to its employees and/or students.
USF System	The University of South Florida System, which comprises three separately-accredited institutions – USF, USF Health, USF St. Petersburg, and USF Sarasota-Manatee – within the State University System of Florida.
Vulnerability	A flaw or weakness in a USF information system security procedures, design, implementation, or internal controls that could be accidentally or intentionally triggered or exploited and result in a security breach or a violation of the system's security policy.

ROLES & RESPONSIBILITIES

These are specific individuals or groups within the USF System and their responsibilities in relation to USF Health information security standards and procedures.

Chief Information Officer (CIO)/Assistant Vice President for Information Technology – responsible for providing information technology management, development, planning, procurement, and implementation activities related to the delivery of quality information services and products for both the business and educational/academic environment.

Director, Office of Information Security, Information Technology (OIS Director)– responsible for University-wide efforts related to data and information system security, such as the development of USF data security policies, negotiation and evaluation of site licenses for security-related software, training, coordination of efforts to improve data security controls, and dissemination of security-related information and incidents, which could affect the availability, and integrity of computing resources on campus.

The Director maintains communications with the other IT Directors, Academic Affairs, Business Systems Reengineering, USF Health IS, Sarasota and St. Pete Directors of Computing, regularly updating them on information security issues that need to be addressed.

Information Security Workgroup (ISW) – a steering committee responsible for recommending policies and assisting in the overall coordination of the University information security program. Chaired by the OIS Director, the ISW advises the ISM on the development and maintenance of standards and guidelines that help other University users and administrators maintain the confidentiality, integrity, and availability of the data they handle. It also assists the OIS Director in evaluating risk analysis surveys completed by individual University units and is responsible for incorporating methods for a systematic, University-wide, risk assessment framework through which appropriate changes in policy, standards, and guidelines are implemented and enforced.

Incident Response Team (IRT) – with a primary goal of protecting the overall computing infrastructure of USF, the IRT is responsible for responding quickly to identify threats to the data infrastructure, assess the level of risk, and take immediate steps to mitigate risks considered significant and harmful to the integrity of USF information system resources. IRT members notify the appropriate department leads of any

incident involving their resources. The IRT consists of the OIS Director and key members of the campus network administration and security staff.

System Administrator (SA) – in accordance with USF Policy #0-501: Using and Protecting Information Technology Resources, employees outside IT may be responsible for the general management of IT resources in certain circumstances. Those individuals are designated as SAs. In terms of data security, their responsibilities include but are not limited to:

- Ensuring that users are aware of and adhere to all USF system security policies and standards;
- Ensuring that the resource meets all information security requirements, including the performance of continuous risk analysis and planning for business resumption in the event of technology failure;
- Helping to promote security awareness within the USF unit
- Advising the OIS Director of security shortfalls.

STATEMENT OF POLICIES, STANDARDS & PROCEDURES

USF IT recognizes that system security is a crucially important aspect of any information system, as it is the only way to safeguard protected data and other sensitive information, to identify and eliminate security threats, and ensure compliance with mandated security requirements. Appropriate security standards and controls will be performed at all stages in the life cycle of any USF information system.

USF System Policies

0-501: Using and Protecting Microcomputing Resources

This policy defines the basic set of procedures that colleges and departments shall establish and maintain for the management, use, and security of their microcomputing resources. It establishes guidelines for the administration of computing resources, control of access to data, software installation and maintenance, business resumption, and personnel training.

0-502: Appropriate Use of Information Technology Resources

Policy outlining acceptable use of the University computing resources. This is a general policy that specifies and gives examples of what is considered misuse of resources and the actions that can be taken in case of misuse.

0-506: Telecommunications Resources Management

The System Vice President, Information Technology, is charged with the responsibility for overseeing the acquisition, planning, installation, modifications, maintenance, repair, relocation and removal of all communication facilities, services, systems and devices that support the USF System, except for specific entities who operate under additional federal regulations that would not usually be applicable to the educational environment. Information Technology handles all network/telecom infrastructure for the entire university system.

0-507: Data Management

Information is an integral part of the business and academic functions of USF System; consequently, data is an important institutional resource. In order to make appropriate decisions, Institutional Data must meet basic standards. It also must be accurate and verifiable. The value of the data maintained by the USF System increases through its widespread and consistent use, and it diminishes through misuse, misinterpretation, or unnecessary restrictions on its access.

0-508: University Information Security Structure

Due to the continued proliferation and distribution of computing and information systems across the entire University,effective structure must be distributed, and a consistent program for addressing security is required. The purpose of this policy is to define the overall information security structure which will ensure the confidentiality, availability, and integrity of all critical University data and information systems.

0-509: Call Accountability

Set forth the authority and responsibility that is delegated to all departments for the establishment and ongoing maintenance of authorization codes required to make chargeable long distance calls accounting for their associated charges and monitoring use of calling.

0-512: Information Technology Governance Structure

This policy specifies charges for several committees, including the Information Technology Management Council, CIO Council and University Technology Standards Board, and advisory groups Cyber-Infrastructure Council, USF Classroom Technology Committee, Identity and Access Management Program Functional Committee, Information Security Workgroup, Council on Technologies for Instruction and Research, Student Technology Advisory Council, Research Computing Advisory Committee, Course Management Advisory Group, Student Information Systems Advisory Board, GEMS/FAST Advisory Group

0-515: Protection of Electronic Personal Information

Define the policy, process, procedures, and requirements that all persons and entities shall follow for the security and protection of personal identity information that is stored electronically at the University. The policy relates to the storage and access of personal identity information and the protections required, not the usage of personal or private data which is covered by other policies and statutes.

0-516: USFID-SSN Appropriate Use Policy

Mandates elimination of the use of the Social Security Number as the primary identifier in information systems and establishes an increased confidence by the USF System community that Social Security Numbers are handled in an appropriate and confidential manner reducing the risk of identity theft.

0-517 USFCard and ID Badge Policy

The USFCard is used for identification, verification of USF System status, use of USF System services such as the library services, door access, purchase of parking decals, obtaining passes for USF System sporting and theatrical events, and other related events and services. This policy addresses the issuance of official USF System identification cards (USFCard) and ID Badges.

0-518: Technology Acquisition Policy

Policy created to standardize technology related items purchased for the University. It establishes the University Technology Standards Board to oversee the creation of standards for the purchase of certain technology resources such as desktop computers. It also establishes levels of approval needed for purchases above a cost threshold.

0-520: Mass Electronic Communication Policy

The purpose of this policy is to articulate the USF System's position involving the use of mass communications using e-mail (sometimes called "bulk e-mail"), SMS (Short Message Service), MMS (Multimedia Message Service), Instant Messaging, and other electronic means to distribute official messages to members of the USF System community.

Standards and Procedures

ISSP-001 - Sensitivity and Criticality of Data

The measures in place to adequately ensure the security of electronic data depend on two parameters: the sensitivity of the data, and the level of criticality of the data. The equipment housing this data inherits the level of criticality and sensitivity of the information it contains. This equipment can be a server,desktop computer, or a backup tape. This document offers guidelines for the classification of electronic resources within the University of South Florida according to their level of criticality and sensitivity.

ISSP-002 - Incident Response and Investigation

Document outlines the procedure involved when responding to security-related incidents at the University, from the time the incident is discovered until it is resolved, and mitigating controls put in place.

ISSP-003 - Active Directory Settings

Password management settings for accounts in the USF System domain.

ISSP-004 - Removal of Network Access

USF must take immediate action to mitigate any threats that have the potential to pose a serious risk to the campus network, campus computers or the Internet. This document outlines circumstances in which machines connected to the USF network would have connectivity shut off due to a security incident..

ISSP-005 - Choosing Strong Passwords

Passwords are the first line of defense on any system connected to the network. It is not enough to have any password associated with an account. Passwords must be chosen in such ways that the casual hacker would not gain access to the account only by trying a few easy combinations. This document provides guidelines to help users pick strong passwords.

ISSP-006 - Securing Sensitive Computers

All computers connected to the network must be appropriately protected. Computers used at USF which contain information considered restricted require additional measures of security. This document outlines

the recommended steps System Administrators must take during the initial setup and ongoing maintenance of such computers.

ISSP-008 - Wireless Network Installations

This document covers wireless system installation standards that must be followed to ensure USF's campus-wide wireless offerings are compatible, provide mobility between locations, and prevent unauthorized access.

ISSP-009 - Media Disposal

Restricted data, such as proprietary information and student information, may reside on various types of media throughout the University. Due to technological advancements, simple deletion or formatting does not provide complete protection of sensitive data. This document contains approved methods for ensuring the confidentiality of USF System Institutional Data when media is disposed.

ISSP-012 - Data Protection Standards for Mobile Devices

Document lists the requirements that must be in place in order to use mobile devices at the University, including but not limited to whole disk encryption.

ISSP-013 - Request for Storage of PII on a Mobile Device

Form used when requesting to utilize a laptop or mobile device to store Personal Identifiable Information.

ISSP-014 - Request for Storage of Social Security Numbers

Form used to request permission to store Social Security Numbers. All USF units that need such storage must first fill out this form and obtain approval from the ISW and CIO groups prior to storing the data.

ISSP-015 - Server Address Assignment and ACL Requests

In order to improve the security posture of the servers part of the IT SVC Data Center and Winter Haven Data Center, the IT's Office of Information Security, in conjunction with Communications Infrastructure and the Data Center Infrastructure group have established a set of network procedures to be followed when setting up a server. This document includes these procedures.

ISSP-017 - Application Owner and Vendor Questionnaire

A questionnaire to be completed prior to the purchase of applications which involve additional work by other IT units during implementation. This questionnaire allows IT to prepare for future projects, but also ensures that USF Institutional Data is protected, equipment used is redundant, determines the criticality and sensitivity of the system, etc.

ISSP-018 - SQL Update Request and Approval Process

Process required to implement SQL changes on data. The primary areas of concern are PeopleSoft and Banner databases. Direct SQL modifications to the data circumvent application level controls in place to log and protect the data. This process ensures the request is documented and properly approved prior to execution.

Security concerns in system management

Recognizing that security is a crucial element in managing the information systems and resources under its control, USF IT will follow a method of system development life cycle (SDLC)[1] planning in its management of those systems, employing recognized security principles[2] during all phases of each system's life cycle.

USF IT standards and procedures for system management, including guidelines for incorporating these security principles into SDLC planning and supervision, are described in more detail in the USF security standards procedures which are detailed at the USF IT web site Technology Acquisition page.

For all information technology acquisitions, including purchase or lease of hardware, software, communication, and peripheral devices, as well as consulting and other technology services, USF system units will follow the policy and procedures established, published and maintained by the USF Vice President for Information Technology through the University Technology Standards Board (UTSB), as described in:

- USF Policy 0-518: Technology Acquisition Policy
- The USF Procurement Process

System access and use

Any policies or procedure developed by any USF business unit, will comply with the official policies, standards and procedures governing user account creation, system access, personal information protection, and the appropriate use of information systems and resources that have been found for the USF System, as described in:

- USF Policy 0-501: Using and Protecting Information Technology Resources
- USF Policy 0-502: Appropriate Use of Information Technology Resources
- USF Policy 0-515: Protection of Electronic Personal Information
- USF Security Standard ISSP-006: Securing Restricted Computers

Supported software

USF IT will only provide technical support for software that has been authorized by USF IT prior to its installation. Any software that is installed without the authorization of USF IT will not be supported. For information, see the USF IT Web page.

System and data integrity

It is the responsibility of USF IT to ensure that USF Business systems (???) perform as intended without unauthorized manipulation, changes or disruptions, and that information residing on those systems can only be accessed or modified by those authorized to do so. USF IT will abide by best practices to safeguard the integrity of its systems and the information that resides on those systems, including:

Control of physical environment

USF IT will help protect system and data integrity in the physical environment by:

- ensuring that servers are accessible only to system/network administrators;

---

[1] As described in Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST Special Publication 800-14, September 1996.

[2] As described in Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication SP 800-27, Rev A, June 2004.

- keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped;
- protecting hardware and storage media from environmental hazards, such as heat, dust, power surges, electrostatic discharges, and magnetism.

System/network administration activities

System and network administration measures to ensure system and data integrity include:

- controlling system access and maintaining current authorization levels for all users,;
- restricting access to sensitive data and maintaining a rigorous authentication practice;
- documenting system/network administration procedures, parameters, and maintenance activities;
- creating and maintaining a disaster recovery plan with contingency strategies for dealing with occurrences such as natural disasters, power outages, server failure, virus attacks, and other emergency situations;
- testing software updates, security controls, and disaster recovery procedures.

Data classification and restriction

Regulations, such as those imposed by official USF system policies or HIPAA and other federal or state legislation, require that certain information stored on a USF Health information system be assigned a security classification and that access to that information is restricted. The security classification assigned to the data is based on its sensitivity and its level of criticality.

USF will follow the guidelines for classification and restriction of electronic data and resources set down in:

USF Security Standard ISSP-001 Sensitivity and Criticality of Data

Risk management

USF IT will manage risk by identifying, evaluating, controlling, and mitigating vulnerabilities that are a potential threat to the data and information systems under its control; it will execute its defined risk management process on an ongoing basis, periodically assessing risks and implementing new controls in response to changes in its information systems as well as to changes to federal, state, and USF regulations and policies.

- Risk assessments will be performed on all new systems or on systems undergoing significant change before they are moved into active production stage, and appropriate measures will be taken to address the risks associated with identified vulnerabilities.
- Annual risk assessments will be performed on active production information systems, and appropriate measures will be taken to address the risk associated with identified vulnerabilities.
- Vulnerability or threat notifications from vendors and other appropriate sources will be monitored and assessed for all systems and applications associated with any USF information system.
- When required, security authorization for USF information systems to operate with security risks that have been evaluated and determined to be acceptable will be obtained from the OIS Director.

Security incident response

USF System units will follow the standard and procedures for responding to security incidents involving its information systems as set down in USF Security Standard ISSP-002: Incident Response and Investigation. This standard outlines the procedures that will be taken in response to incidents involving data security throughout the USF System, including:

- Incident reporting

- Containment
- Notifications
- Investigation
- Final report/recommendations

Incidents involving data and/or resources considered to be "restricted," as defined in USF Security Standard ISSP-001: Sensitivity and Criticality of Data, will be communicated to the USF Information Security Manager immediately upon the occurrence.

As an ongoing process, USF IT will keep track of both positive and negative results of its responses to security incidents and incorporate the lessons learned into its incident response procedures and training activities.

Security awareness and training

All USF employees must be aware of, have access to, and comply with USF information system security policies, standards, and procedures.

USF staff may be required to have training, depending on job duties and access to restricted information.

Resources for USF security awareness and training include:

- USF Security (main website)
- USF Security – Official Policies
- USF Security – Standards and Procedures
- USF Security – Monthly Security Information Awareness Newsletter

Security audits

USF IT will ensure that annual internal security audits are conducted on USF information systems and resources. The intent of a security audit will be to verify adherence to the standards and procedures set down in the USF IT Security Plan and ensure that a given information system has appropriate and adequate controls in place to safeguard USF assets, maintain data integrity, and operate effectively and efficiently to meet the objectives of the USF organization.

EXCEPTIONS

All requests for exceptions to the USF IT Security Plan:

- Must be submitted in writing to and approved by the OIS Director. If approved, the request will be forwarded to the CIO for consideration.
- An exception will not be permitted unless written approval is obtained.
- Will be reviewed on a case by case basis.

Approved exceptions will be reviewed annually and cancelled as required.