Information Security Consulting

SERVICE CATEGORY

Information Security Consulting

SERVICE UNIT

Information Security Office

DESCRIPTION

This service will have the Information Security Office (ISO) work with colleges and departments to develop a strong security culture through consultation with the Departmental Security Coordinator (DSC.) ISO will assist in managing information technology assets securely and proactively. You may request for ISO to develop and implement specific security controls for new or existing projects, systems or processes. If security concerns or issues arise, ISO will assist the department with proper steps and mitigation techniques. ISO will also assist colleges and departments when cloud services are considered to replace or augment IT operations.

FUNCTIONALITY LIST

N/A

TECHNICAL SPECIFICATIONS

N/A

INCLUDED SERVICE COMPONENTS - OVERVIEW:

Department Security Coordinators (DSCs) who serve as a communication liaison for campus IT security

OPTIONAL SERVICE COMPONENTS - OVERVIEW:

None

ESTIMATED PRICE	PRICE TERMS	RECURRING	Nonrecurring Charge (setup)	SIGNED SLA REQUIRED
$0	Per Hour	Monthly	0	False

AUTHORIZED CUSTOMERS

All UCF departments, organizations, faculty and staff

SERVICE AVAILABILITY LOCATIONS

All UCF campuses and Research Park

SERVICE OWNER

Information Security Consulting

Computer Forensics

SERVICE CATEGORY

Security Incident Handling

SERVICE UNIT

Information Security Office

DESCRIPTION

With this service, the Information Security Office (ISO) uses analytical and investigative techniques to identify, collect, examine, and preserve evidence or information that is stored or encoded on business systems. The goal is to provide digital evidence of a specific or general activity. This service is usually requested in response to administrative/HR investigations such as inappropriate computer use, violation of the UCF acceptable use policy, incident assessment, and unauthorized (accidental or intentional) disclosure of university data. ISO closely works with the National Center for Forensic Science (NCFS) and UCF law enforcement with regard to forensics investigations. Forensic analysis services may aid in the completion of a pending investigation. At the request of the department head and authorization from the VP, ISO will perform an in-depth analysis of an employee's computer, limited to the scope of questions originally proposed.

FUNCTIONALITY LIST

N/A

TECHNICAL SPECIFICATIONS

N/A

INCLUDED SERVICE COMPONENTS - OVERVIEW:

Provide detailed reports based on criteria of the administrative investigation.
Customers who would like to request this service will need to fill out this form:

http://www.cst.ucf.edu/wp-content/uploads/Request_for_Forensic_Examination.docx

OPTIONAL SERVICE COMPONENTS - OVERVIEW:

None

ESTIMATED	PRICE	RECURRING	Nonrecurring	SIGNED SLA

PRICE	TERMS		Charge (setup)	REQUIRED
$0	Per Hour	Monthly	0	False

AUTHORIZED CUSTOMERS

All UCF departments, organizations, faculty and staff

SERVICE AVAILABILITY LOCATIONS

All UCF campuses and Research Park

SERVICE OWNER

Incident Handling

Information Security Incident Response

SERVICE CATEGORY

Security Incident Handling

SERVICE UNIT

Information Security Office

DESCRIPTION

The Information Security Office (ISO) is responsible for organizing an information security incident response capability to detect incidents, minimize loss, and mitigate exploited vulnerabilities to restore service. ISO and Security Incident Response Team (SIRT) will work alongside IT departments, management, and law enforcement to handle incidents from initial preparation through the post-incident phase. ISO and SIRT are designed to carry out incident response procedures on Denial of Service (DoS), malicious code, unauthorized access, inappropriate usage, and multiple component attacks involving malicious code that might lead to unauthorized access. ISO will also aid in notifying proper authorities regarding the incident response and remediation.

FUNCTIONALITY LIST
N/A

TECHNICAL SPECIFICATIONS
N/A

INCLUDED SERVICE COMPONENTS - OVERVIEW:
Request for Service at

http://www.cst.ucf.edu/about/information-security-office/incident-response/

OPTIONAL SERVICE COMPONENTS - OVERVIEW:
None

ESTIMATED	PRICE	RECURRING	Nonrecurring	SIGNED SLA

PRICE	TERMS	One-Time	Charge (setup)	REQUIRED
$0	Per Service		0	False

AUTHORIZED CUSTOMERS

All UCF departments, organizations, faculty, staff and students

SERVICE AVAILABILITY LOCATIONS

All UCF campuses and Research Park

SERVICE OWNER

Incident Handling

Absolute Software Management Service - Asset Recovery Tool

SERVICE CATEGORY

Security Incident Handling

SERVICE UNIT

Information Security Office

DESCRIPTION

This service provides centralized management of UCF's CompuTrace service. CompuTrace is designed to track, manage, and recover mobile computers and compatible devices for better data protection, easier IT asset management, and computer theft recovery. CompuTrace will allow departments to work with ISO to remotely locate stolen computer assets for recovery purposes, and when necessary implement remote data delete. It is strongly recommended for mobile devices containing restricted data.

FUNCTIONALITY LIST

N/A

TECHNICAL SPECIFICATIONS

N/A

INCLUDED SERVICE COMPONENTS - OVERVIEW:

Provide support for Absolute Software's CompuTrace Product, e.g. creating department group, creating customer center account, providing the ability to do remote data delete

OPTIONAL SERVICE COMPONENTS - OVERVIEW:

N/A

ESTIMATED PRICE	PRICE TERMS	RECURRING	Nonrecurring Charge (setup)	SIGNED SLA REQUIRED
$0	Per Service	One-Time	0	False

AUTHORIZED CUSTOMERS

All UCF departments, organizations, faculty, and staff

SERVICE AVAILABILITY LOCATIONS

All UCF campuses and Research Park

SERVICE OWNER

Information Security Consulting

Security Risk Assessments

SERVICE CATEGORY

Security Risk Management

SERVICE UNIT

Information Security Office

DESCRIPTION

This service offers departments a general security assessment based on the National Institute of Standards and Technology (NIST) which may include vendor risk assessments (VRM), vulnerability assessments, web application assessments, compliance to regulations or contracts, such as FERPA, PCI DSS, HIPAA, etc., and general recommendations for reducing IT risk to an acceptable level thereby protecting the department's ability to perform their mission.

FUNCTIONALITY LIST

N/A

TECHNICAL SPECIFICATIONS

N/A

INCLUDED SERVICE COMPONENTS - OVERVIEW:

Conduct assessments of systems to ensure they are appropriately secured and meet all applicable standards and regulations regarding the security of information

OPTIONAL SERVICE COMPONENTS - OVERVIEW:

None

ESTIMATED PRICE	PRICE TERMS	RECURRING	Nonrecurring Charge (setup)	SIGNED SLA REQUIRED
$0	Per Hour	Monthly	0	False

AUTHORIZED CUSTOMERS

All UCF departments, organizations, faculty or staff

SERVICE AVAILABILITY LOCATIONS

All UCF campuses and Research Park

SERVICE OWNER

Security Risk Management

Security Awareness and Education

SERVICE CATEGORY

Security Risk Management

SERVICE UNIT

Information Security Office

DESCRIPTION

This service provides educational awareness sessions tailored to UCF faculty, staff, and students through the Information Security Office (ISO.) After completing the session, individuals with no previous security awareness will understand important concepts in information security, such as phishing threats, understanding strong passwords, and safe data handling practices.

FUNCTIONALITY LIST

N/A

TECHNICAL SPECIFICATIONS

N/A

INCLUDED SERVICE COMPONENTS - OVERVIEW:

General security information to IT, annual security day conference, annual security information to the community, etc.

OPTIONAL SERVICE COMPONENTS - OVERVIEW:

None

ESTIMATED PRICE	PRICE TERMS	RECURRING	Nonrecurring Charge (setup)	SIGNED SLA REQUIRED
$0	Per Service	Yearly	0	False

AUTHORIZED CUSTOMERS

All UCF departments, organizations, faculty, staff and students

SERVICE AVAILABILITY LOCATIONS

All UCF campuses and Research Park

SERVICE OWNER

Security Risk Management

Secure LDAP Authentication

SERVICE CATEGORY

Identity Management

SERVICE UNIT

Information Security Office

DESCRIPTION

The LDAP authentication service authenticates users to a NET Domain joined server or application using their NID username and password.

Secure LDAP queries provide a hub for applications to obtain directory information from, which can then be used for authorizing users of an application, populating forms, or a variety of other actions in the central username directory (i.e., Net Domain). The domain currently provides the following information: name, department, enterprise email, employee work telephone number, security, and distribution groups, etc. Secure LDAP queries are only allowed on standard secured port 636 and all data is updated daily based on feeds pulled from multiple sources. Anonymous bind is not permitted.

FUNCTIONALITY LIST

Provides centralized sign-on authentication to domain joined systems using the central username directory.

TECHNICAL SPECIFICATIONS

The service uses secure LDAP to pass authentication and authorization information to an integrated application. No write access is permitted. The database is read-only.

INCLUDED SERVICE COMPONENTS - OVERVIEW:

Connection to the central username directory is provided along with a service account and access control list.

OPTIONAL SERVICE COMPONENTS - OVERVIEW:

N/A

ESTIMATED	PRICE	RECURRING	Nonrecurring	SIGNED SLA

PRICE	TERMS	Yearly	Charge (setup)	REQUIRED
$0	Per Installation		0	True

AUTHORIZED CUSTOMERS

NET Domain departmental users authorized to manage on premise web applications.

SERVICE AVAILABILITY LOCATIONS

All

SERVICE OWNER

Identity Management

Electronic Federated Identity (EFI) Sign-on Service

SERVICE CATEGORY

Identity Management

SERVICE UNIT

Information Security Office

DESCRIPTION

Electronic Federated Identity (EFI) Service uses UCF federated login services to authenticate UCF users to on-site and contractual partnered (cloud) services via the central username directory.

UCF uses Shibboleth software to host an Identity Provider (IdP) capable of authenticating users against the central directory using their NID and NID password. Once authenticated, the IdP sends the userID back to the application along with any unique computed value(s) or an attribute(s) from the directory. Applications can use these attributes to identify the type of user authenticating to the system.

Once a user authenticates using EFI, they will be able to log into other Service Providers (SP) defined in the IdP without an additional login (timeout limited).

FUNCTIONALITY LIST

Allows for central signon authentication based on the central NID directory.

TECHNICAL SPECIFICATIONS

The service uses SAML2 version, or higher, assertions to pass NET domain NID authentication information to the application. The most compatable Service Provider can be implemented with the Shibboleth SP open source code. Information about the Shibboleth SP can be found at http://shibboleth.internet2.edu/documentation.html.

INCLUDED SERVICE COMPONENTS - OVERVIEW:

Connection to the Identity Provider (IdP) Interface for web applications.

OPTIONAL SERVICE COMPONENTS - OVERVIEW:

UCF is a member of the InCommon Federation. As an option Service Provider (SP) metadata for an application set up to authenticate to UCF IdP can be published to InCommon to be added to the federation metadata. This would allow the application to accept authentication from any IdP in the InCommon Federation.

ESTIMATED PRICE	PRICE TERMS	RECURRING	Nonrecurring Charge (setup)	SIGNED SLA REQUIRED
$50	Per Installation	Yearly	50	True

AUTHORIZED CUSTOMERS

Departmental users authorized to manage a UCF web site.

SERVICE AVAILABILITY LOCATIONS

All

SERVICE OWNER

Identity Management