Information Security Services Operating Standards

1 INTRODUCTION

The purpose of this document is intended to reflect a strong commitment by the Information Services division and its staff within Information Security Services, to achieve the highest standards of quality, professional customer service, enable ease of accessibility, and effective event resolution for Central Washington University.

1.1 LOCATION

The Information Security Services (ISS) office is located at Samuelson, Room 255.

1.2 CONTACT US

- Security Services is available by phone via the Service Desk at 509-963-2001 during hours of operation.
- Assistance is also available via email at security_services@cwu.edu
- Incidents can be reported via email at https://www.cwu.edu/security-services/cwu-security-incident-report
- Specific staff contact information is available on the security webpage at https://www.cwu.edu/security-services/staff

1.3 HOURS OF OPERATION

Normal hours of operation for Information Security Services are Monday – Friday from 8:00 AM until 5:00 PM. Information Security Services follows the same holiday schedule approved for the staff of Central Washington University.

1.4 STANDARDS & BEST PRACTICES

- ITIL (Information Technology Infrastructure Library) is a standardized set of best practices that CWU's Information Services (IS) Department uses to align IT processes and procedures.
- The ISO/IEC 27000 family of information security standards, which is developed and published by the International Organization for Standardization and International Electrotechnical Commission, and is a core standard used in ISS. The standards provide a globally recognized framework for best-practice in information security.
- The NIST Framework was published in 2014 by the US National Institute of Standards and Technology is used as a security baseline to promote the protection and resilience of critical infrastructure at CWU. It consists of standards, guidelines and best practices to manage cybersecurity related risk
- CWU uses Best Practices which are ever-evolving as new ideas, technology, and information comes to light. Information Services and Security Services is committed to using all the knowledge and technology at our disposal to ensure success.

2 SUPPORTED SERVICES

Information Security Services is dedicated to protecting Central's information systems and data, while establishing a culture of information assurance and privacy. Information Security Service's offered are listed below;

2.1 ERP SUPPORT (HR/Financials/CatPlan/Campus Solutions)

- Account Provisioning/ De-Provisioning
- Role & Permissions Engineering
- System Enhancements, Upgrades, Integrations and Fixes

2.2 INCIDENT MANAGEMENT

- Students, faculty, and staff shall immediately report potential incidents to their supervisor or Security Services department or designated office, as defined below. The incident reporting form is available on the Security Services website
- See the diagram listed below for the high level incident management process flow:

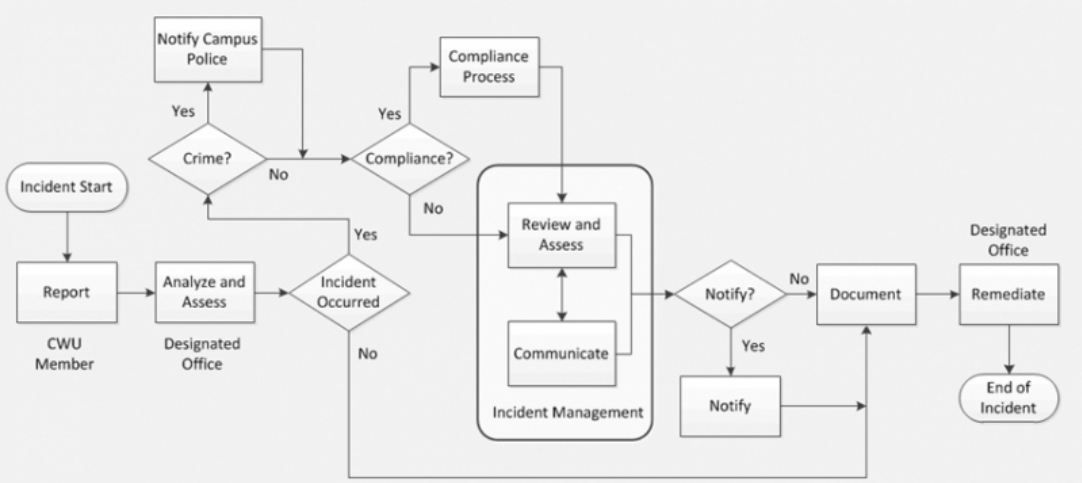

Figure 1: High Level Incident Management Process Flow

2.3 AUDIT

- Logical Access Audit
- Infrastructure & System Audits
- Compliance Audit

2.4 COMPLIANCE & RISK MGT

- PCI
- HIPAA
- FERPA
- Risk and Security Assessments

2.5 NETWORK SECURITY

- Vulnerability Scans
- System and Log Analysis
- IDS
- Penetration Tests

2.6 DIGITAL FORENSICS

- Preservation, identification, analysis, extraction, and documentation of computer evidence for internal CWU investigations. For legal cases it is recommended that departments contact the Attorney General's office.
- Windows Devices

- Macintosh Devices (Coming soon)

2.7 SECURITY AWARENESS EDUCATION

- National Events
- Speakers
- Tabling
- 1:1 or Small Team Training
- Simulated Phishing
- Social Media * Newsletters * Posters

2.8 POLICY & PROCEDURES

2.9 PROJECT SUPPORT

3 SERVICE LEVEL GUIDELINES

Information Security Services supports student, faculty, and staff support calls and web submissions made through the TD ticketing system.

3.1 3x3 STANDARD

Information Security Services follows a 3x3 rule; after a ticket has been submitted and has insufficient information or is waiting on follow-up, or the customer cannot be contacted, ISS will make a second attempt to contact the customer to obtain the necessary information. After 3 business days, if ISS has not received a response from the customer, Security Services will notify the customer that in 3 additional business days the ticket will be reassigned to them. This will be as an effort to have the ticket show up in the work queue of the person who is currently responsible for some action or information. When done, the ticket can be reassigned back to Information Security Services.

3.2 INFORMATION TECHNOLOGY SERVICE MANAGEMENT WORKFLOW

Customer service is the focal point of all IS priorities. The CWU Information Security Services team (ISS) uses Information Technology Infrastructure Library (ITIL) as the framework to achieve high quality service. The teams are trained in several areas of ITIL and currently use Incident, Service Request and Problem tickets to restore service to the customer.

There are two types of services: Internal and External. The definitions are:

- Internal Ticket: defined as a ticket generated by the Information Services (IS) staff for internal task completion. Internal tickets can be opened, resolved and closed

by internal staff or, alternatively, left resolved for the Service Desk to close.

- **External Ticket**: defined as a ticket generated by the customer through the Service Desk Catalog. The external ticket may also be generated by the customer through the Service Desk technicians. All external tickets will escalate to the respective department as needed, including IS Security Services.

The ITIL definition of Incident, Service Request and Problem tickets are:

- **Incident:** a ticket generated for the purpose of restoring a service to its original state as quickly as possible.
- **Service Request**: a ticket generated for the purpose of adding a feature or service as requested by the customer or IS staff.
- **Problem:** a ticket generated for the purpose of a root cause analysis of an incident series of incidents

3.3 INCIDENT RESPONSE SLAs

If an incident is identified that requires escalation to the next level of support, the table below outlines our standard service level commitments. All Priority 1 and 2 tickets will be managed personally by the Service Desk Manager and escalated by a phone call or personal delivery to the department manager escalated to.

Priority	Definition	Service Response to Customer	Resolved or workaround Time
1	Critical [Emergency] – An incident impacting a significant group of customers, any mission critical IT issues affecting a single customer, or potential loss of mission-critical data.	15 Minutes	59 Minutes
2	High – An incident where the user or multiple users' performance is significantly interrupted or that interferes with core business functions.	30 Minutes	2 Hours

3	Medium – An incident that interferes with normal completion of work, tasks are more difficult but not impossible to complete, or the incident affects a small group of users. This priority allows the technician to respond when available without loss of productivity. This is the default priority.	4 Hours	16 Hours
4	Low – An incident that does not directly affect customer's productivity, and work can continue until the technician responds.	8 Hours	32 Hours

3.4 TICKETS ON HOLD

On Hold ticket process:

Criteria for placing a ticket on hold.

1. Waiting on customer, parts/equipment or support from external resource.
2. Scheduled to take place at a date in the future, such as a check-out, hire or termination

Analysts can place a ticket on hold if it meets any of the criteria's listed above. If the analyst is given a future date by the customer/vendor/technician, they will assign it a start date and an end date if applicable. If an end date is assigned the analyst will also assign a "goes off hold" date.