SUNY Potsdam
Administrative Unit
Assessment Summary Form

Administrative Unit: Computing & Technology Services	***Unit Contact Name:*** Mindy Thompson	***Date:*** *July 27, 2023*
Phone: *x3486*	***Email Address:*** *thompsme@potsdam.edu*	***Assessment Year:*** 2022-2023

PURPOSE

This annual assessment summary form provides the opportunity for units to follow-up on their assessment plans, track progress toward goals, and to highlight actions taken to improve processes and/or efficiencies in functioning that lead to outcomes that benefits students, staff, or the college. These could be process changes or improvements in efficiency, skill level of staff, opportunities for the college, or other aspects over which the unit has a certain amount of control.

SECTION 1: ASSESSMENT PLAN FOLLOW-UP

A key component of the continuous improvement assessment process is regularly following up on your assessment plan. Please review your plan and select one-third of your unit goals, along with related desired outcomes and objectives to report on the progress made.

Selected Goal

Copy/Paste or enter the goal(s) from your unit plan that you wish to highlight and summarize.

Continue to develop computer labs and support on-campus technology facilities to integrate the most current technologies. Ensure that the facilities meet the student and faculty needs for current activities and are capable of being changed to meet future technological requirements.

Desired Outcomes/Objectives

Copy/Paste or enter the desired outcomes and objectives connected to your selected goal that you will be reporting on.

1. Effectively communicate lab access and availability to current students (Outcome 3A).
2. Generate maps displaying available computers and software in each facility (Outcome 3B).
3. Enhance current facilities through appropriate upgrades and maintenance (Outcome 3C).

Related Targets/Measures

Copy/Paste or enter the target desired outcomes and objectives connected to your selected goal that you will be reporting on.

1. Utilize KeyReporter to map facilities accurately and publish facility hours and computer access information on the College website. Track page views using Google Analytics. Target: Increase traffic to lab hours page by 5% annually.
2. Utilize KeyReporter to display available computers and software in each facility. Target: Ensure all facilities are mapped and accessible through KeyReporter.

3. Track device age, current operating system, and utilization using computing asset management software (AllSight). Target: Implement a five-year equipment replacement plan and perform annual upgrades as necessary.

Describe the progress made toward the selected goal and the related desired outcomes and objectives. Be sure to include steps taken and any information/data collected and results.

This annual assessment provides an overview of the progress Computing & Technology Services made in developing computer labs and supporting on-campus technology facilities to integrate the most current technologies. The objective is to ensure that these facilities meet the needs of students and faculty for current activities while remaining adaptable to future technological requirements.

Review of Goals:

1. **KeyReporter Implementation:**
   - All facilities are now mapped and available for public view and access through KeyReporter.
   - Software analytics reports within AllSight have been organized to enable viewing available software within each facility.
   - Google Analytics implementation for tracking page views has not yet been completed due to competing staff priorities.

2. **Computing Asset Management (AllSight):**
   - Device age, operating system, and utilization tracking goals have been met.
   - No set computing lifecycle plan is currently in place due to financial constraints.
   - Approvals have been obtained to replace two primary student computing facilities with outdated computers.
   - One facility upgrade request is pending with the finance team.

Based on the assessment data and information shared above, what planned actions were or will be taken as a result?

Insights and Recommendations:

1. **Communication and Accessibility:**
   The implementation of KeyReporter has successfully allowed students and faculty to access lab hours and computer availability information. To further improve engagement, Computing & Technology Services will need to prioritize the completion of Google Analytics implementation in KeyReporter to track page views and monitor website traffic.
2. **Facility Upgrades:**
   Despite financial constraints, the successful replacement of outdated computers in two primary student computing facilities demonstrates progress. It is important that Computing & Technology services continue advocating for necessary upgrades and replacements to ensure the facilities remain equipped with current technologies that meet the evolving needs of students and faculty.

3. **Financial Considerations:**
Given the current financial challenges, it is understandable that implementing a set computing lifecycle plan may not be feasible. However, we will need to focus ongoing efforts to secure necessary funding for regular upgrades and replacements, prioritizing areas with the highest need and impact on student learning experiences.

Moving forward, the Department of Computing & Technology Services will need to maintain a strong focus on integrating current technologies, regularly assessing facility needs, and seeking resources to support upgrades and maintenance. This will ensure that computer labs and technology facilities continue to meet the evolving demands of students and faculty, both in the present and future.

SECTION 2: ADDITIONAL ASSESSMENT ACTIVITY

Please use this space to share an example from this past year when you used assessment and data to plan and/or take action. Be sure to include any available information relating to the results and impact. Your example for this section does not need to be directly tied to your previously submitted administrative unit assessment plan.

During the 22 – 23 academic year, Computing & Technology Services (CTS) went through a multipart process to create a robust Cyber Security Incident Response Plan. The plan was designed to address the increasing cyber threats and align with New York State and Federal guidelines for cyber security. Through campus-wide participation, involving stakeholders in Student Affairs, Academic Affairs, University Police, College Communications, Computing and Technology Services, Environmental Health and Safety, Human Resources and our FERPA Officer, in a SUNY-driven tabletop exercise, CTS identified vulnerabilities and developed strategies to enhance cyber security, ensuring continuity of critical campus services in the face of potential cyber incidents.

Key Developments and Initiatives

Framework for Security Assessment:
CTS established a framework to assess campus security and ensure compliance with evolving cyber security guidelines at the state and federal levels. The framework acted as a roadmap to guide the creation of an effective Cyber Security Incident Response Plan.

Campus-wide Tabletop Exercise:
Participation in the SUNY-driven tabletop exercise allowed for a comprehensive assessment of the campus's cyber security posture. This exercise identified potential risks and vulnerabilities, offering insights into critical campus services that could be impacted by a ransomware attack.

Development of Alternate Planning:
Based on the tabletop exercise findings, CTS developed alternate planning strategies to increase service availability during a major cyber attack. This included evaluating the hosting of campus services, both in the cloud and on premises, to ensure continuity and resilience.

Internal Process Review:
CTS conducted an internal review of cyber security practices and processes. This review led to necessary adjustments, enhancements, and refinements to internal practices, strengthening the overall cyber security infrastructure.

Handling of Cyber Security Events:

CTS successfully managed the assessment and handling of three distinct cyber security events on campus, each offering unique insights to improve incident response capabilities and enhance the Cyber Security Incident Response Plan (CSIRP).

1. **Compromised End User Device:**
   In the first event, CTS received a passive monitoring alert indicating a compromised end user device. Responding swiftly, the device was immediately collected, and a thorough reimaging process was executed to remove the malicious software. Simultaneously, the network underwent a comprehensive scan to assess the extent of the compromise. The rapid response and effective containment prevented any further spread of the threat beyond the initial device. Throughout the incident, the CSIRP was utilized, allowing for a detailed review and assessment. This event highlighted the importance of process documentation, revealing areas for improvement within the CSIRP to strengthen future incident responses.
2. **Breach at the National Student Clearing House:**
   The second event involved a breach at the National Student Clearing House, resulting in the interception of student data. With the CSIRP in action, CTS promptly assessed the potential impact on campus areas and implemented the necessary monitoring processes. Additionally, clear documentation ensured that all reporting requirements to State and Federal agencies were met in a timely and organized manner. The incident response demonstrated the plan's efficacy in facilitating efficient coordination and compliance during external security incidents.
3. **Third-Party Software Assessment:**
   The third event concerned a third-party software that SUNY Potsdam no longer utilized. Through rigorous investigation, CTS determined that the software posed no risk or impact on campus systems. This event served as an opportunity to further refine the CSIRP, emphasizing the importance of continuous assessment and thorough evaluation even in cases of software no longer in active use.

Campus Training Assessment:
Also in the 22-23 academic year, CTS developed required compliance training and assessments for faculty and staff to empower the campus community in cyber security awareness. These compliance trainings address various cyber threats such as phishing, spoofing, ransomware, and the importance of secure password creation.

Documented Department-Level Processes:
CTS created and documented department-level processes for cyber security event assessment. This standardized approach allowed for consistent incident response.

Impact and Recommendations

The development of a comprehensive Cyber Security Incident Response Plan has significantly strengthened SUNY Potsdam's cyber security readiness. The initiatives undertaken by CTS, involving many other offices on campus in the process, have fostered a culture of cyber security awareness and proactive response across the campus community. Notable outcomes include improved incident handling capabilities, enhanced service availability, and heightened resilience against cyber threats.

The successful handling of the aforementioned cyber security events exemplifies the effectiveness of the CSIRP in guiding timely and well-coordinated responses. Each event provided valuable insights to enhance incident response capabilities and identified areas for improvement. The CSIRP's agility and adaptability have proven vital in safeguarding campus data and systems against diverse cyber threats.

Recommendations for further improvement

Ongoing Training and Awareness:
Continuously reinforce cyber security training and awareness programs to keep the campus community informed about emerging threats and best practices.

Regular Plan Review and Testing:
Conduct periodic reviews and testing of the Cyber Security Incident Response Plan to ensure its effectiveness and alignment with evolving cyber threats.

Collaborative Approach:
Foster collaboration with other campus units to ensure a coordinated and unified response to cyber incidents.

Fiscal Resources:
Prioritize cyber security in allocating institutional resources, including OS upgrades, computer hardware renewal, endpoint security solutions, cyber security training, data encryption, access controls, incident response, cybersecurity audits, and assessments.

In conclusion, the development of the Cyber Security Incident Response Plan demonstrates SUNY Potsdam's commitment to safeguarding its digital assets and maintaining the continuity of critical services. The ongoing efforts by CTS to enhance cyber security practices and engage the campus community in cyber awareness are essential to maintaining a secure and resilient environment in the face of evolving cyber threats.