SERVICE DEFINITION
Version 4.0 – October 18, 2019

INFORMATION TECHNOLOGY
Security Operations

Coordinate security operations initiatives and provide security tools and processes across the UW System

DESCRIPTION OF THE SERVICE

UW-Shared Services will, in collaboration with leadership from UW System Administration and institutional IT departments, establish a security operations group that consistently deploys security tools and protocols across UW institutions. UW-Shared Services will install and/or configure the Cisco security tool suite (Umbrella, Cloudlock, AMP for End Points, and Stealthwatch) for use by UW institutions to implement in their environments. If requested, UW-Shared Services will assist institution security staff with the implementation of these tools.

SOURCE OF THE SERVICE

Institutional visits, the UW System IS Strategy/Work Plan, and feedback from: Chief Information Officers/IT Directors, and UW System Administration

UW-Shared Services will establish a common set of security processes for monitoring, response and reporting requirements; coordinate security and vulnerability management initiatives; coordinate and support a System-wide asset management program; monitor security breaches; track security issues; administer the System-wide phishing campaigns; and implement a security log analysis program. The institutional IT departments will be responsible for implementing these processes and tools at their institutions, and UW-Shared Services will monitor the success of ongoing security initiatives to learn and adapt the standard processes.

UW-Shared Services will also promote good security processes and raise security awareness among UW employees through communication campaigns and trainings.

FORMS OF THE SERVICE

ACTIONS

On-Demand	●	UW institutions may request consultation, tool implementation, and incident response services from UW-Shared Services as needed.
Ongoing	●	UW-Shared Services will manage ongoing security initiatives including campaigns, tool maintenance, and special projects.
Monitoring	●	UW-Shared Services will monitor and report on issues that arise across UW institutions related to phishing, attacks, and breaches.

STANDARDS

Practices	●	UW-Shared Services will establish standard information security processes and tools for use across UW institutions.
Trainings	●	UW-Shared Services will provide virtual security training for employees of UW institutions and track completion rates through the *Human Resources: Mandatory Employee Training* service.
Systems	●	UW-Shared Services will manage the Cisco security tool suite, specialized security tools, and enterprise systems for ticketing and communications.

SUPPORT

Passive	●	UW-Shared Services will provide information and guidance on information security to UW institutions.
Distance	●	Customers will be able to ask for support and guidance on information security by calling or contacting the UW-Shared Services IT help desk.
In-Person	○	UW-Shared Services only plans on providing information security support remotely; institutions would provide on-site security support.

ANALYSIS

BENEFITS	RISKS
• Decreases financial, regulatory, legal, and reputational risk through standardization and consistency • Reduces efforts to replicate security tools and processes across institutions • Relatively inexpensive to scale across institutions • Eases the burden on institutional IT departments	• May cost some institutional IT departments to switch to the new security processes and tools • Could reduce incident response time if not implemented appropriately and with adequate communication channels

PARTICIPATION MODEL

The *Security Operations* service should be mandatory for all comprehensive institutions given the need to mitigate the high risk posed by information security breaches, issues, and hacks for UW institutions. There have been several high-profile security breaches and incidents in American higher education, so the severity and probability of UW facing such security risks is relatively high. Standardizing processes, tools, and training across UW institutions, and advocating for information security measures should help mitigate that risk.

RECOMMENDATION
MANDATORY PARTICIPATION For UW System comprehensive institutions and UW System Administration

Also, considering the scale that UW-Shared Services can achieve from offering these processes and tools, and the relatively low upfront costs of developing the service, it would be reasonably inexpensive and easy to expand access to these security operations across all UW institutions. Given the ease with which this service could be expanded across UW institutions and the risk associated with non-compliance, this service should be mandatory for all UW institutions.

FUNDING MODEL

The *Security Operations* service should be funded by UW-Shared Services base funding, although base funding of the service does not include the annual cost of the Cisco tools. Institutions should not be charged directly for this service, given the need to incentivize the use of these security operations and eliminate any potential barriers.

Given the high risk associated with information security issues and breaches, UW-Shared Services should ensure that institutions use this service as much as possible. Charging the institutions could create disincentives to using the security operations tools and processes, which would limit the benefits of this service for the UW System.

RECOMMENDATION	
TRANSACTIONAL CHARGEBACKS	**BASE FUNDING + CHARGEBACKS**
CAMPUS ASSESSMENT	**BASE FUNDING** This service should be funded by UW-Shared Services base funding

Allocating base funding for this service should establish the appropriate incentives across the institutions to fully utilize these security tools and processes and should limit the administrative effort required to manage the funding model.