Saint Mary's University
2024-25
Priorities and Target Allocations
of the
Research Security Funds

Research Security Priority / Vision:

Saint Mary's has an integrated approach to Cyber Security that includes research computing. Our CIO Enterprise Information Technology (EIT) department work with the Office of the AVP-Research to provide cyber security solutions that support and protect research activities both on campus and out to the broader community at large. Our program is achieved through the 3 components "People / Process / Technology" as described below.

PEOPLE:

We have assigned resources that support the inventory, deployment and security configuration across our research cluster and researchers in the field, from both a Hardware and Software (HW, SW) perspective.

PROCESS:

Our research community members participate in the university cyber security awareness training. The research network and attached devices are subject to regular vulnerability and penetration testing by both third-part and internal scans. We subscribe to security operation centre monitoring services like the CANSSOC and the ACORN-NS/CANARIE SIEM.

TECHNOLOGY:

We have deployed a virtual sandbox environment separated by V-Lan that is controllable through the research firewall which provides a secure environment where research can be conducted without performance impact from our normal detection and filtering solutions. In further support of research continuity, an air-gapped Google environment has been provisioned and implemented to support the resurrection of research data and systems backup.

With this approach, we will continue to enhance the protection of our systems and data through our Zero Trust initiative. This is a multi-year, multi-layered approach to cyber security for our whole institution.

Saint Mary's University

Research Security Fund – 2024-25 Target Allocations:

Saint Mary's has an Research Security Fund allocation of **$10,633** for 2024-25.

This amount will be targeted toward two projects in support of the overall vision.

1. Microsoft Sentinel SIEM tools ($5,633)

   With the addition of security tools, comes an increase in the signals and data that must be analyzed. At present our staff must monitor multiple systems and this data resides within our institution. We are piloting Microsoft Sentinel SIEM tools that will collate all these cyber security signals into a single system that will enable our staff to monitor, analyze and respond. Additionally, by anonymizing some of this data and collaborating with other institutions, we are confident this dataset could be shared with other institutions to provide enhanced protection for Research across multiple institutions. We anticipate this SIEM investment will require an annual commitment of around $36k in cloud costs. The portion of Research Security funds allocated to this project will be split between subscription costs and staff training.

2. Cloud Firewall ($5,000)

   As our research community continues to take advantage of the ability to work from any device, anywhere, at any time, it is vital that our Cyber Security tools can support and protect this flexible research model. During FY24-25 we are investing $60k into a toolset that will extend the same Cyber Security features and functionality that traditionally only existed on campus, out to all of our research community wherever they are located. This toolset will provide remote connectivity to secured Research Systems and Data, provides Endpoint Detection and Response tools, Web Security Gateway and Data Loss Prevention. Adding these additional layers to our security model whilst minimizing disruption to our researchers. The portion of Research Security funds allocated to this project will be split between subscription costs and staff training.