Saint Mary's University
2026-27
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.

Research Security Fund – 2026-27 Target Allocations:

Saint Mary's has an Research Security Fund allocation of **$15,759** for 2026-27.

This amount will be targeted toward this project in support of the overall vision.

- Managed Detection and Response Service ($15,758)

  The University is implementing a third party service (Bell Cyber) to provide 24x7 monitoring and response to the University networks and server environment including research. This service includes periodic vulnerability assessments of the Saint Mary's secure environment. This is a 24 month pilot project.

  Project started at beginning of FY27 (April 1, 2026) and anticipated to complete after 24 months.

  During FY27 and FY28, it is anticipated that approximately $77,000 will be invested toward this important project – and the $15,759 from the Research Security Fund will supplement this amount during FY27.