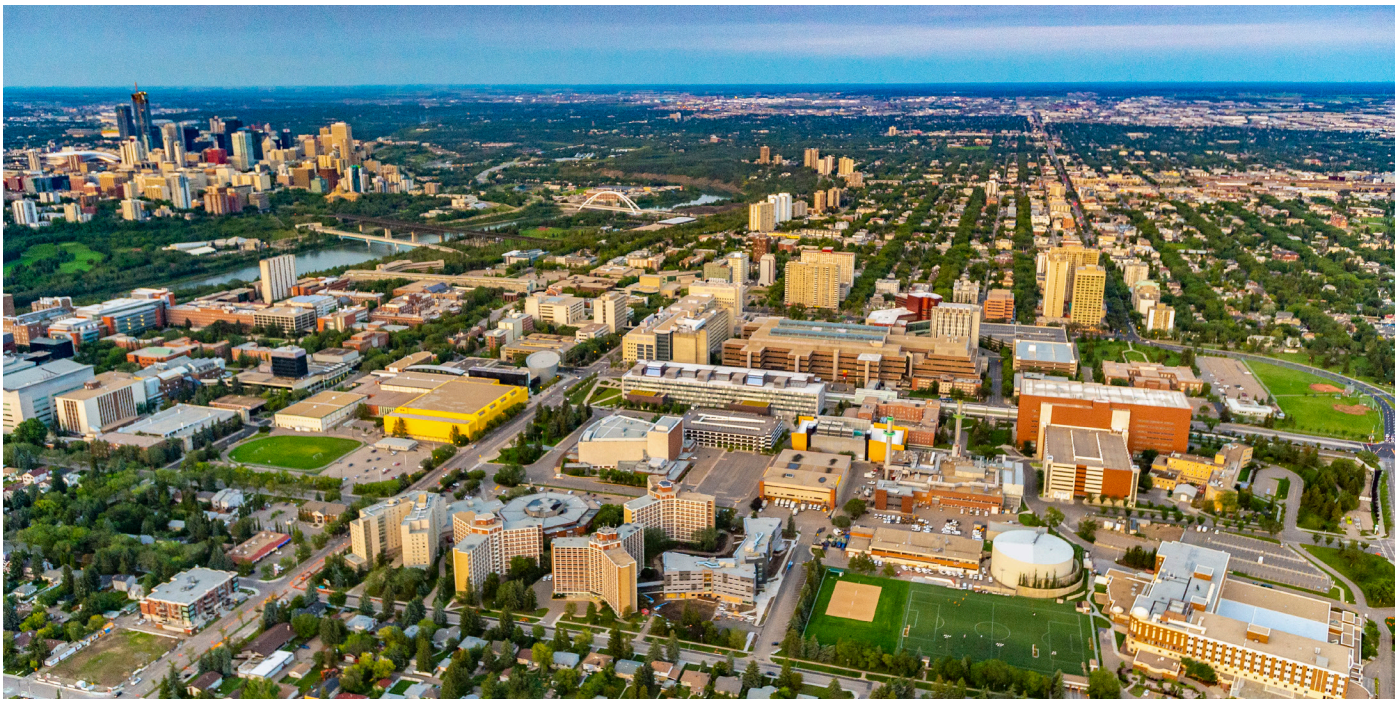
UNIVERSITY OF ALBERTA

What We Heard Report
IT Policy Redevelopment

MARCH 6, 2025



Contents

Introduction

This report summarizes the feedback collected during the IT Security Policy redevelopment roundtables held between December 2024 and February 2025. The roundtables were organized and led by the Information Services and Technology (IST) and sought to gather input from the university community to refine policy statements, clarify principles, and define roles and responsibilities. The feedback has been categorized under key themes that align with the revised IT Security Policy structure.

This document provides a high-level summary of key concerns and recommendations shared by the university community. It is not a comprehensive report but a guiding document for shaping the final policy.

Engagement Process

CONSULTATION APPROACH

A working group was formed to oversee the consultation process and ensure broad participation. Planned engagement activities included audience-based roundtable discussions and targeted meetings with key university committees.

PARTICIPATION SUMMARY

Roundtable discussions

To gather meaningful feedback on the proposed IT Security Policy statements, principles, roles and responsibilities, IST organized a series of roundtable discussions, starting with an internal IST session held on November 26, 2025.

Researcher roundtables

The first external roundtables were targeted at researchers, with sessions held on Dec.4 and 13, 2024 and Jan.15 and 22, 2025. Over 50 invitations were sent to researchers across campus, resulting in 19 participants who provided valuable insights into IT security needs specific to research environments.

Administration and leadership roundtables

The second phase of discussions engaged members of university administration and leadership. A total of 41 people were invited to participate in three roundtables held on January 13, 16 and 30, 2025. Of those invited, 27 registered.

Community-wide roundtables

The final phase included open community-wide roundtables, allowing all interested university members to contribute. These sessions were scheduled for Feb.12, 19 and 27, 2025. A total of 33 people registered and participated in these three roundtables.

Additional feedback opportunities

To ensure broad input, all invitees across sessions were provided an opportunity to submit feedback via email, allowing for asynchronous participation and broader engagement in shaping the policy. A follow-up email prompting them to provide additional feedback in writing allowed for two more weeks to do so from the date of the email. A few individuals and groups appreciated the opportunity and contributed their additional notes.

Key Findings

Most attendees participated to listen and understand the direction of the policy development. There was broad agreement on the need to balance policy standardization with minimizing disruptions to operations. Specific concerns were raised about how the policy might affect research data and associated security measures.

The following key themes emerged:

POLICY ACCESSIBILITY AND CLARITY

Roundtable participants found UAPPOL confusing, difficult to navigate and cluttered with conflicting policies and outdated links, which made finding the right information challenging. For instance, some policies, such as procurement and IT equipment policies, contradict each other, creating confusion for end users. It was also noted that policies and procedures are lengthy, which made the intuitive location of relevant information within documents difficult.

Several participants emphasized the importance of keeping procedural details separate from policies to maintain flexibility when seeking procedural approvals.

IT SECURITY POLICY PRINCIPLES

Most principles were well-received; however, some participants struggled with Principle 4[1] and suggested rewording for clarity and conciseness.

A section for applying policies was suggested to provide structured guidance on decision-making.

[1] With mobility and remote teaching, learning, researching, and working from anywhere, anytime, on any device, the concept of the "trusted university network" is antiquated and the university must adapt its information security accordingly.

Participants emphasized the need for concise, clear language in policy around the Bring-Your-Own-Device (BYOD) option and unmanaged IT systems.

Interest in a cybercommunity of practice was expressed, but overall, participants prefer engagement when the topics are directly relevant to their work.

Participants emphasized the importance of clear definitions to ensure consistency across university policies. Concerns were raised about inconsistencies in terminology, particularly in defining "information" and "IT infrastructure", as different disciplines may interpret these terms differently.

There was also support for more substantial security awareness initiatives, particularly in recognizing phishing and other cyber threats. Hosting a one-time impactful campaign based on real-life breach examples was suggested as a more effective alternative to ongoing initiatives.

POLICY STATEMENTS

The need for precise definitions was highlighted, including clarification on what constitutes an IT resource.

Participants emphasized the importance of a robust data classification system to assess and mitigate security risks.

Two policy options were discussed:

Option 1

(Decentralized with exceptions) was preferred for its flexibility, particularly by researchers needing specialized IT solutions. Ensuring clear security controls and university oversight was suggested and well received.

Participants noted that research needs are too varied for a centralized IT structure. Concerns were raised about vague terminology such as "wherever feasible" and how exceptions would be handled. It was suggested that the policy explicitly mention the individuals responsible rather than using broad terms like "college, faculty, department, and unit."

Option 2

(Centralized IST oversight) was largely seen as overly broad and impractical given research-specific needs.

Concerns were raised about IST's capacity to manage all IT infrastructure effectively due to the diversity of IT needs across research, teaching, and administration. It was noted that a centralized model could delay access to specialized IT solutions due to budget and staffing constraints, negatively impacting research operations. A suggestion was made that the policy ensures that non-IST IT services are still recognized as institutional rather than being classified as external or non-institutional. Some noted positive experiences with central IT support but suggested that success stories should be communicated more effectively. A hybrid approach was largely preferred, where IST oversees cybersecurity while allowing localized control for specific research needs.

Participants also emphasized the need for explicit security controls and accountability measures when exceptions to IST-managed infrastructure are required.

ROLES & RESPONSIBILITIES

The need to explicitly outline student responsibilities within IT security policies was identified. It was noted that research staff, including Research Assistants (RAs) and Teaching Assistants (TAs), are often overlooked in policy discussions.

Policies should distinguish between accountability (decision-making) and responsibility (execution) with a clear delegation of duties.

Policies should ensure clear distinctions between faculty, staff, and researchers to avoid gaps in accountability. Embedding roles directly in policy may be too rigid; instead, role definitions could be embedded in procedural documents that allow for updates as responsibilities evolve.

Clear definitions and expectations for research groups managing their IT infrastructure should be included.

A strong recommendation was made for ongoing security training tailored to researchers, particularly in system administration and secure computing environments.

There was a call to streamline onboarding and offboarding processes, incorporating automating to ensure security compliance.

Faculty and departmental authorities should have clearer mandates for enforcing compliance with security policies.

Stakeholders expect the Chief Information Officer (CIO) & Chief Information Security Officer (CISO) to provide clear direction on compliance, risk management and incident response.

BALANCING SECURITY & USABILITY

Excessive security controls can reduce usability and adoption. Security measures should be user-friendly and not impede productivity. There were concerns about cumbersome authentication processes, such as multi-factor authentication prompts, which may impact workflow efficiency.

Policies should focus on managing risks rather than implementing blanket security measures that may not be relevant across all university functions.

Participants supported increased and mandatory cybersecurity training emphasizing storytelling and real-life case studies to enhance engagement.

There is an ongoing challenge of balancing open access to research data with necessary security measures. Funder requirements and disciplinary needs are critical.

IMPLEMENTATION

Participants supported developing a security council to oversee security decisions, address implementation challenges, and ensure continuous engagement. They also noted that an effective governance model must recognize the complexity of university-wide IT infrastructure while maintaining a high level of responsibility for departmental needs.

Policies should reflect the needs of both administrative and research communities, with specialized provisions where necessary.

Policies should include diverse perspectives, including Indigenous knowledge systems and community needs.

Participants advocated for a streamlined one-business-day standard for security-related approvals, flexible for complex cases.

Many research units require Linux support, raising questions about whether IST should provide specialized support or guidance on maintaining security compliance.

A call was made to establish a clear reporting structure for security concerns, ensuring compliance does not become overly bureaucratic or burdensome.

Recommendations

Ensure that IT policies and supporting procedures are easy to find and read.

- Consolidate related policies and remove conflicting provisions
- Create clear, structured policy rubrics for application

Establish clear policy and guiding principles

- Clarify principle 4[2] to make it more actionable
- Strengthen language around data classification and IT resource definition
- Address BYOD concerns explicitly within the policy framework

Refine policy statements

- Adopt a hybrid security model combining centralized oversight with local flexibility
- Clearly define exceptions and ensure a structured process for approvals
- Avoid vague language such as “whenever feasible” and instead outline concrete expectations

[2] With mobility and remote teaching, learning, researching, and working from anywhere, anytime, on any device, the concept of the “trusted university network” is antiquated and the university must adapt its information security accordingly.

Clarify roles and responsibilities

- Define student roles in IT security policy
- Clearly distinguish between accountability and responsibility
- Ensure faculty and department administrators have clear mandates for IT security compliance

Improve security awareness and training

- Launch a high-impact one-time cybersecurity awareness campaign with real-world breach examples
- Implement ongoing but targeted training initiatives, integrating security principles into existing research and teaching frameworks
- Develop a cybersecurity community of practice for interested stakeholders

Establish governance and implementation structures

- Establish an IT security oversight committee to ensure continuous engagement and policy alignment
- Engage Associate Deans (Research) in integrating security considerations into existing approval processes
- Improve IST communication and responsiveness to build confidence among faculty and researchers

Ensure inclusive and practical implementation

- Address unique research needs, including specialized software and hardware requirements
- Align policies with external partners, such as AHS, where applicable
- Incorporate Indigenous perspectives and diverse user experiences into IT security frameworks.

Conclusion

The IT Security Policy redevelopment roundtable engagements highlighted a strong desire for policies that are clear, actionable and supportive of both security and operational needs. While participants recognized the importance of robust security measures, they also stressed the need for usability, flexibility and transparency.