

Informed IT

April 2025
Quarterly Newsletter

The Faculty of Information IT newsletter

INSIDE

Why Secure Tools Matter

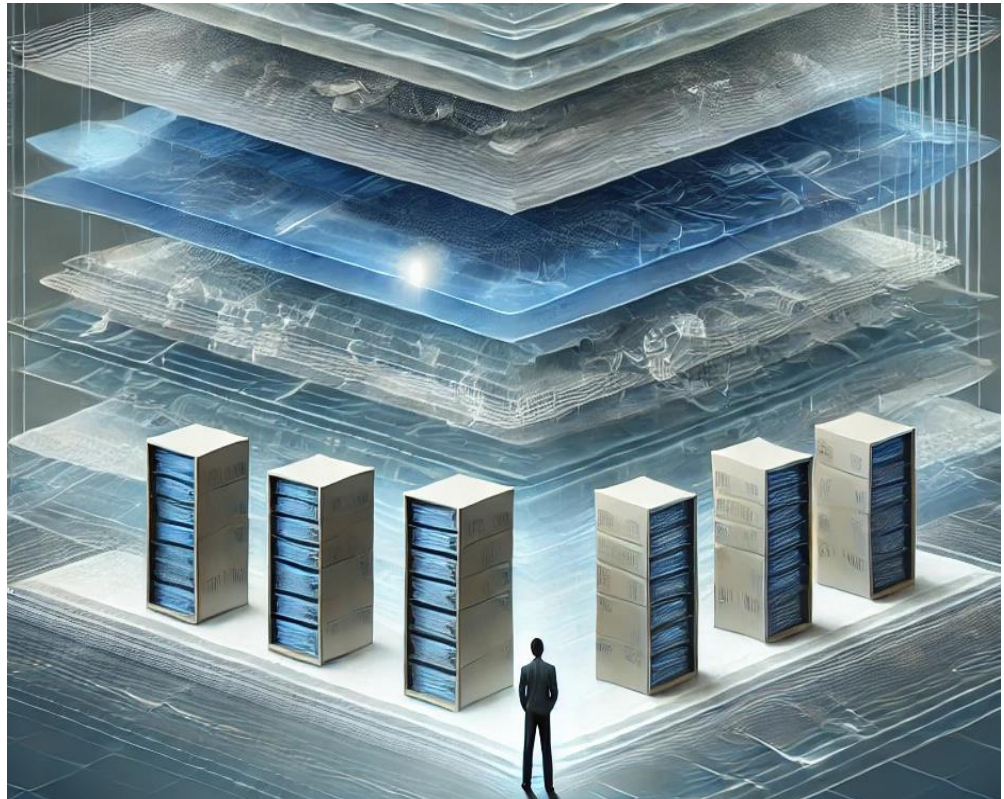
A Reflection on Data,
Design, and Stewardship

IT Services at the faculty of Information

Our newly launched
services, available for use.

Meet the team

Meet the individuals who
help make things happen



Informed IT is a quarterly newsletter designed to keep the Faculty of Information up to date on key issues and activities within the Information Technology space here at the Faculty and University. Tailored specifically for faculty and staff, it covers a broad range of topics that impact on how we work. Each issue dives into topics of interest that can range from the philosophy of data that intersects with IT (ethics, ontology, privacy, AI), to more practical matters like cybersecurity and compliance - highlighting current threats, safe computing habits, and proactive measures being taken on by the IT team to provide services and protect our students, systems and data. Our goal is to provide relevant and useful information with the hope to inspire conversations and enhance productivity, streamline workflows, and support academic needs. We also welcome feedback and topics to expand our perspective and goals.

Importantly, *Informed IT* offers a human context by sharing the perspectives of the Faculty's IT team: what we are working on, lessons learned from recent projects, and tips based on real-world challenges. Our hope is to bring to life the "why" behind the tech to build a collaborative and living community of informed partners in knowledge to help build an exceptional IT experience at the Faculty of Information.

Why Secure Tools Matter:

A Reflection on Data, Design, and Stewardship

By Alex DiMarco - Manager, Technical Services

I've spent my career in IT, but this article isn't so much about technology but about the choices we make, and what those choices say about our values. At the iSchool, we ask hard questions about data. That means also asking hard questions about the tools we use every day: *Who controls the data? Who benefits from it? And what's really at stake?*

Too often, decisions about technology are made for convenience, cost, or convention and the consequences are buried in the fine print. This is evident in recent news such as the massive data breach at 23andme triggering the bankruptcy and sale of the company placing the DNA of 15 million people up for grabs to the highest bidder. How did 15 million peoples' personal data get harvested, repackaged, and now sold? Did the users ever realising what they signed up for? Would they have clicked the agreement if they knew that their data could be purchased by their insurance company to possibly evaluate their eligibility as a client for coverage? These aren't abstract risks; they're baked into the majority of systems that are in use today.

This is one of the many reasons why the IT team is focused on providing tools that truly protect privacy not only to meet regulatory requirements such as FIPPA but by making deliberate choices to support faculty with privacy-first, ethically designed tools to help keep research safe. We believe that truly secure systems aren't just safer—they're more aligned with our mission to empower people, protect communities, and design for the public good.

In *Unseen Layers: A Personal Take on Data and IT Practice*, I explore how my time in the field has shaped my view that good systems design is ethical design. Privacy isn't just a feature. It's a foundation. This is why the tools we choose matter. And this is where responsible systems design begins. My full article is available to be read on the IT support blog (<https://support.ischool.utoronto.ca/unseen-layers-a-personal-take-on-data-and-it-practice/>).



IT Services at the faculty of Information

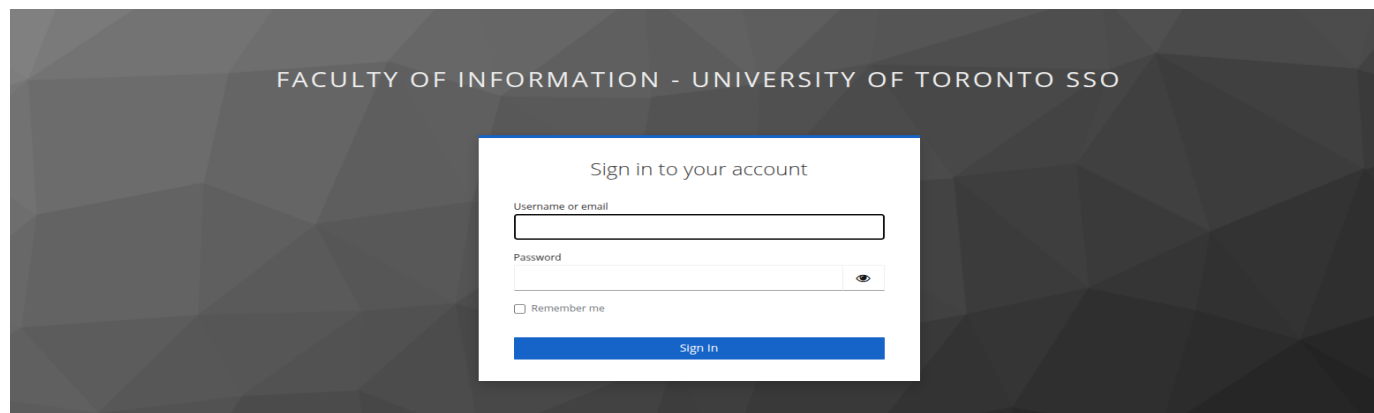
Where we started.

Over the past two years, we've invested in a dedicated cluster of servers hosted at the University of Toronto Library data center to support the evolving IT and operational needs of the faculty. Central to this is our Proxmox hypervisor cluster—a virtualization platform that enables us to efficiently run and manage multiple virtual machines across our infrastructure. We've launched a new email server, ticket system, inventory system and a Mailman 3-based groups server to serve as the communications backbone for the faculty. In addition, we've built out a secure internal network and integrated a suite of security tools to ensure robust access control, monitoring, and data protection. For classroom and academic support, we've deployed services as needs have arisen, including MariaDB for database-driven classes, a MASA server for media

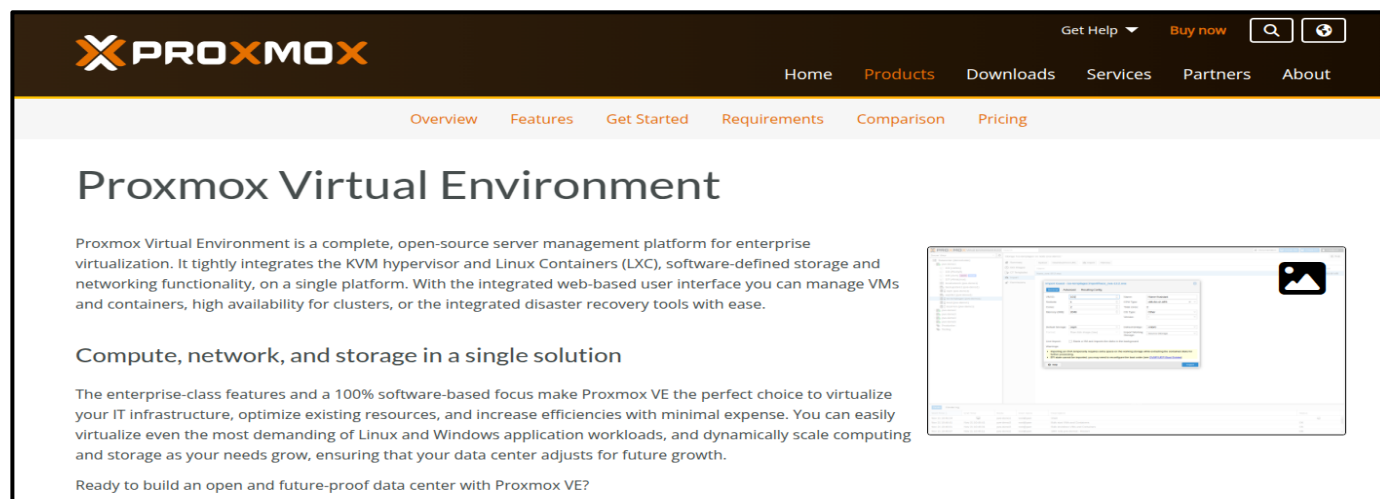
access, Atom and Archivematica for archival management, WordPress sites for flexible publishing, and an Omeka server for digital exhibits. These tools are helping us deliver targeted, scalable services to Faculty, Teaching, and Staff.

We have recently expanded the available IT tools - here are our newest additions.

Many collaboration tools and file storage tools in the industry are not designed for personal privacy and self-data ownership. This has led to several privacy-first projects that continue to rise. At the faculty we have made available the following to help address some of these issues.



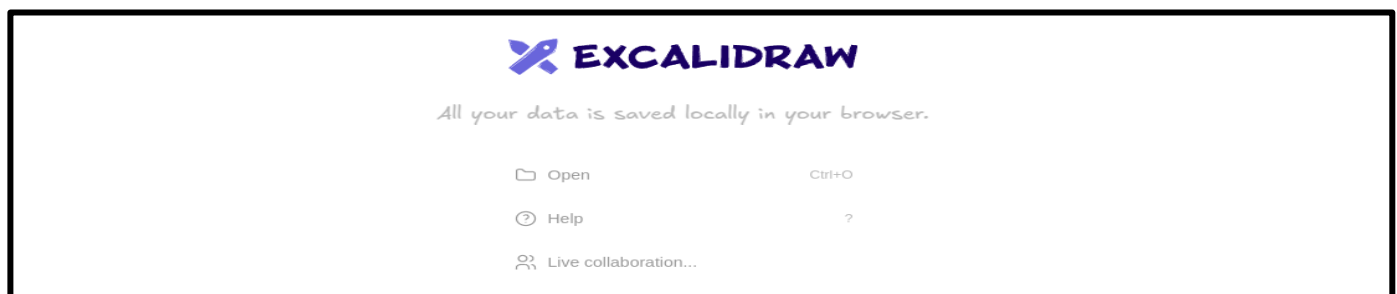
Keycloak—a solid, open-source tool for managing logins, was originally built by Red Hat and is now part of the Cloud Native Computing Foundation (CNCF), which backs some of the most trusted tools used in real-world, high-security systems across the world. With Keycloak in place, students, staff, and external partners can now access all Faculty of Information tools and resources through one secure login. It also boosts security across the board by supporting two-factor authentication (2FA), making it much harder for accounts to be compromised. Whether you are doing research, teaching, or working on a project, access is flexible to all stakeholders and situations and easier due to integration with our platform. Soon we will be integrating our solution with the University's EntraID system to provide seamless access for stakeholders integrated within the U of T system while still allowing external partner access in situations which require it.



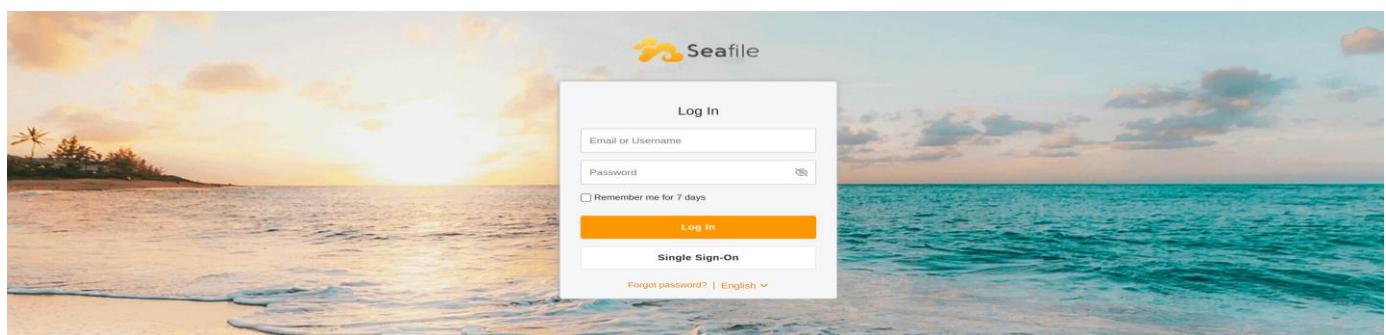
At the Faculty of Information, we use [Proxmox](#) as our hypervisor platform to power our servers and deliver virtual machine (VM) services. Integrated with our Single Sign On, Proxmox is a powerful, open-source solution trusted by IT teams worldwide for managing VMs and containers with flexibility and reliability. It lets us spin up secure environments for teaching, research, and development. Whether you are in need to test out software, a researcher running experiments, or a PI working with an external partner on a project, Proxmox helps us provide fast, stable, and secure access to the resources you need—while giving you the flexibility to work with whoever you need, no matter where they are or whether they're officially part of the Faculty.



CryptPad is a privacy-focused, open-source collaborative platform that empowers users to create and share documents securely. Unlike traditional tools, CryptPad offers end-to-end encryption, ensuring that only users have access to their data. Its user-friendly interface supports a range of applications, including chat collaboration, calendaring, documents, spreadsheets, and presentations. Ideal for teams and individuals valuing data security, CryptPad makes collaboration fast and accessible while maintaining privacy. Whether brainstorming, drafting, or sharing, CryptPad offers a secure space for productive, confidential teamwork. We host this locally and integrate authentication with the Faculty's Single sign on system.



Excalidraw is an open-source virtual whiteboard tool designed for secure, intuitive collaboration. Often seen as a privacy-focused alternative to Miro, Excalidraw enables real-time co-drawing and brainstorming with a simple, hand-drawn style. Its local-first approach ensures that data remains private unless explicitly shared, allowing teams full control over their information. Excalidraw supports end-to-end encryption for shared sessions, making it ideal for confidential projects. With an emphasis on simplicity and security, Excalidraw is perfect for teams seeking a flexible, private space for visual thinking and collaborative planning.



Seafile is our open-source file hosting and collaboration platform configured to use FIPS-140-2 certified encryption (on a hardened Linux system) designed for high performance and security. It enables users to store, synchronize, and share files across devices with robust encryption, including end-to-end encryption (E2EE) for maximum data privacy. Seafile supports granular permission settings, version control, and flexible sharing options, making it ideal for handling sensitive information. Its E2EE function ensures that only authorized users can access encrypted libraries, enhancing data protection during storage and transfer.

New ideas, tools, and projects on the horizon

As we continue strengthening the Faculty of Information's digital infrastructure, several exciting services and tools are currently in development or under review. These initiatives reflect our commitment to privacy-first design, robust classroom support, and responsive research tools.

Virtual Desktop Infrastructure (VDI):

We are exploring the viability of faculty-hosted virtual labs using our Proxmox Hypervisor. These will offer students and instructors access to fully configured virtual machines for classroom software, accessible remotely through our secure login system. This will enable flexible, secure computing for teaching, demo environments, and remote support. TA and instructor roles will have multi-machine visibility for in-class assistance, and we are hoping to explore future integration of proctoring capabilities.

Expanded Teaching and Research Tools:

Following the deployment of CryptPad, Seafile, and Excalidraw, we're exploring additional privacy-forward platforms such as Penpot—a collaborative design tool and open-source alternative to Figma—for UI/UX instruction. We're also exploring the possibility of offering RStudio server access for classrooms that require advanced statistical computing, fully integrated with our SSO and hosted in-house to ensure compliance and scalability.

Secure Print Management:

We are currently piloting Savapage, an open-source print management system that supports secure workflows across all devices. This system is being tested for integration with our authentication services and could offer an equitable, FIPPA-compliant alternative to costly commercial systems, that is printer agnostic.

Accessibility Tools & Teaching Support Expansion:

We are exploring conversations around the discovery and deployment of accessibility software and adaptive hardware for students and instructors. In tandem, we're working on expanding our Teaching Technology Support into a broader Research and Teaching Technology Support (RTTS) initiative. We plan to expand the team's focus on proactive needs assessment and discovery, along with the present focus on classroom reporting and support, to expand our support presence across research and teaching environments.

As always, these services are designed not just to meet regulatory compliance—but to foster a more empowered, equitable, and secure digital environment. Stay tuned.

Operational Design Goals

The Faculty of Information IT team's operational design goal is to support academic needs with robust security at its core, ensuring systems are protected by default. Compliance requirements—often driven by contracts or specific regulatory contexts—are layered on as needed, without disrupting core operations. It's important to distinguish between security and compliance: security is about protecting systems and data from threats, while compliance involves meeting specific legal, contractual, or policy requirements. Our systems are built on strong security foundations to meet the faculty's academic needs, designed flexibly so that additional requirements, such as compliance, can be applied efficiently when required.

We all share the responsibility of protecting personal and confidential information in line with Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) and the new Bill 194. This means being thoughtful about how we handle details that could identify someone—such as student names, emails, ID numbers, academic records, or health-related information, keeping the data safe and within Canada. These protections apply across all formats, from formal documents to emails and even handwritten notes. By being mindful about when and how we access, store, or share this kind of information, and by using privacy-first tools and platforms, we help create a respectful and secure environment for everyone in our community.

For our systems, the key factors we look at are as follows, using Seafile as an example:

Component	Description
 Seafile (FIPS 140-2)	Encrypted storage & syncing
 Keycloak SSO + MFA	Identity & access management
 Wazuh	SIEM, FIM, active threat detection
 Kopia	End-to-end encrypted backups (AES-256)
 Canadian Data Residency	All services and storage located within Canada
 Disaster Recovery (DR) Testing	Routine validation of restores from Kopia
 Internal PIA & IRP	Documented processes for privacy & incident response
 Least Privilege IAM Plan	Defined access roles, separation of duties
 Wazuh Active Intrusion Simulation	Real-time attack detection and alert validation
 Security Awareness & PHI Training	Staff are trained and tracked annually

Requirement	Status	Fulfilled By
Encryption at Rest (FIPS 140-2, AES-256)	✓	Seafile + Kopia
Encryption in Transit (TLS 1.2+/1.3)	✓	Seafile TLS Config
Multi-Factor Authentication (MFA)	✓	Keycloak
Centralized Identity Management (SSO, RBAC)	✓	Keycloak
Audit Logging & FIM	✓	Wazuh
Intrusion Detection (Host-based & File-level)	✓	Wazuh
Active Intrusion Testing	✓	Wazuh active response + test events
Breach Detection & IRP	✓	IRP, Wazuh, Syslog
Backups (Encrypted, Canadian, Tested)	✓	Kopia with DR testing logs
Disaster Recovery Plan	✓	DR runbooks, restore test logs
Privacy Impact Assessment (PIA)	✓	Internal documented PIA
Administrative Safeguards	✓	Policies + training + reviews
Least Privilege Access Model	✓	Role design + audit + SSO config
Data Residency (Canada)	✓	All services hosted in-country
Security Awareness & PHI Training	✓	Annual tracked training

To support this effort, we will be engaging a security penetration testing firm in May to evaluate our Single Sign-On system and validate the integrity of our design to provide staunch support to integrate our system with the university's EntralID.

Meet the IT team

Full-time staff:



Alex DiMarco – Manager, Technical Services

From audio mixing and music to philosophy, IT, and even a stint in theatre, my path has never followed a straight line—and I wouldn't have it any other way. Over the past 25 years, I've worked across multiple departments at the University of Toronto, including Computer Science, Arts & Science, Earth Sciences, and now the Faculty of Information. This broad experience has shaped not only my technical perspective but also my approach to collaboration, communication, and community. I'm driven by curiosity and creativity, whether I'm building systems, solving problems, or crafting the perfect cup of coffee. When I take time to unwind, you'll likely find me by a lake, enjoying good food, tending to a BBQ, and sharing a good conversation as I soak in the moment. I cook without recipes, chase clarity in life and work, and believe the best gift you can give—at home or on the job—is love, time, and inspiration. Every day, I try to live that out... and although I don't always know if I succeed, my hope is that I do, more often than not.



Curtis Debi – Technology Support Specialist

I support Mac, Android, iOS, Windows (and a touch of Linux) using tools like Intune, Ninja One, JAMF, Apple School Manager, and SharePoint. I'm focused on helping people—not just solving problems, but making sure they feel supported, including my peers. Outside of work, I prioritize family, like experimenting in the culinary arts and, always love a strong cup of coffee to keep me running.



Thomas Kiss – Help Desk Analyst and Classroom Support

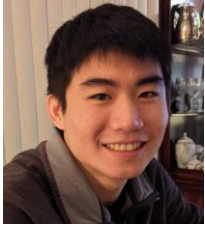
From troubleshooting classroom computers as a kid to navigating IT challenges today, my journey in tech has always felt like second nature. When I'm not problem-solving at work, you will find me deep in a Dungeons & Dragons campaign or passionately lamenting the latest heartbreak from Toronto sports teams. I believe that open and honest communication is the key to success—whether it's in tech support, teamwork, or rolling a natural 20 when it matters most.

Supporting Casual staff:



Hazel Hay – Technical Project Co-Ordinator

As a Master's graduate of the MI program and staff member, my transition from student to staff is a testament to the outstanding teaching and learning environment fostered here at the Faculty of Information. I am naturally empathetic and have always been drawn to helping others. Whether it is leading weekly Uno games at the local assisted living facility or pet-sitting for friends and family, I am most fulfilled when I am supporting those around me.



Hansi Xu - Junior Systems Administrator, Programmer

I am always up for a challenge. I like braving the unknown. This translates to patient problem solving at work, and falling into numerous rabbit holes in my free time; music composition, PC building, language learning... My long-term personal project is developing a game with a meaningful story (and if possible, a shocking twist). If you think you saw a student in a staff-only area, it was likely me.

Supporting special project contractors - Beetree Tech, Meggeson Interactive Technologies:



S. Preston Beach - Sr. Systems Architect

Even though I bring many years of experience from many sectors to the table, I am constantly pushing the boundaries of cutting-edge technology by deploying the latest in technical solutions and keeping my knowledge current. My main skills are figuring things out and empowering people through education. When I am not happily solving difficult tasks at my desk, I enjoy hiking in nature and keeping fit, in both body and mind, through my martial arts practice.



Steve Meggeson - Sr. Microsoft Systems Architect

With over 20 years in IT, I specialize in Microsoft cloud technologies, including Office 365, Azure administration, SharePoint automation, and cybersecurity design. My background includes architecting multi-tenant environments, managing hybrid infrastructures, leading migration projects, and delivering user-focused training at scale. I bring a strong focus on operational efficiency, secure system design, and team mentorship—ensuring solutions are not just technically sound but also sustainable and user-friendly. Recently, I've been recharging with a scuba trip in the Philippines, staying curious both in and out of the cloud.