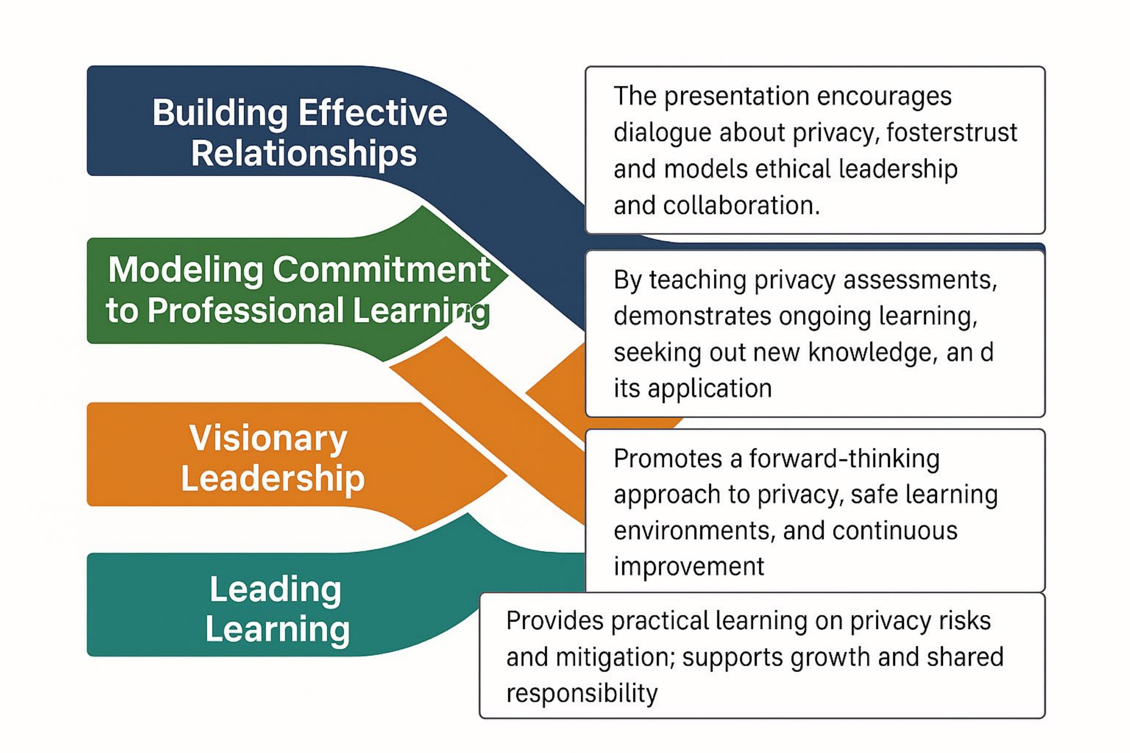
Privacy Impact Assessments: Why They Matter and How to Begin



Building Effective Relationships

The presentation encourages dialogue about privacy, fosterstrust and models ethical leadership and collaboration.

Modeling Commitment to Professional Learning

By teaching privacy assessments, demonstrates ongoing learning, seeking out new knowledge, an d its application

Visionary Leadership

Promotes a forward-thinking approach to privacy, safe learning environments, and continuous improvement

Leading Learning

Provides practical learning on privacy risks and mitigation; supports growth and shared responsibility

By: Jesse Sadlowski

Jesse.sadlowski@lethsd.ab.ca

Goodbye FOIP with Bills 33 and 34

- Welcome the **Protection of Privacy Act** (POPA) and the **Access to Information Act** (ATIA)

- All Public Bodies will be required to have a **Privacy Management Program** (PMP)
    - Required by law
    - Has several components
    - Required to have one in place by June 11, 2026
    - Needs to be accessible to “the public” with one exception for cybersecurity information

PIA Policies will now be a Requirement

Provide information About software, platforms or consistent use service that uses Personal Information.

Must be submitted to the Office of the Information and Privacy Commissioners of Alberta (OIPC) if the software or project or SERVICE includes new or substantial change

Likely based on the Health Information Act (HIA) PIAs, but template from OIPC for public bodies is “coming” in December

Policies and procedures related to [completing and submitting privacy impact assessments (PIAs)]

We conduct Privacy Impact Assessments (PIAs) to identify and understand privacy risks in our systems, helping us decide whether those risks are acceptable and how to mitigate them effectively.

Other reasons

- **Mitigate Privacy Risks Early**
- **Ensure Legal and Regulatory Compliance**
- **Build Public Trust and Transparency**
- **Improve Data Governance and Accountability**
- **Prepare for Future Privacy Challenges**

Have good Polices, procedures and workflows will go a long way in mitigating risks

- **Key Considerations for Privacy Impact Assessments (PIAs)**
- **Leverage Modern IT Tools to Protect Data**
- Utilize the latest technologies to strengthen data security and privacy safeguards.
- **Adopt a Zero Trust Philosophy Organization-Wide**
- Trust no one by default—verify everything. This approach minimizes risk and enhances overall security posture.
- **Implement Automation and Identity Management**
- Streamline access controls and user authentication to reduce human error and improve data protection.
- **Foster Collaborative Practices**
- Cross-departmental collaboration ensures privacy is considered at every stage of system design and implementation.
- **Clarify the Difference Between Security and Privacy Breaches**
- Not all privacy breaches stem from security failures. While every security breach is a privacy concern, privacy breaches can occur without a security incident. These terms should not be used interchangeably.

Remember: Any system connected to our network introduces the potential for lateral movement by attackers. If a security breach occurs, we must assume that private data may have been compromised—even if the breach isn't immediately visible.

What is Lateral Movement

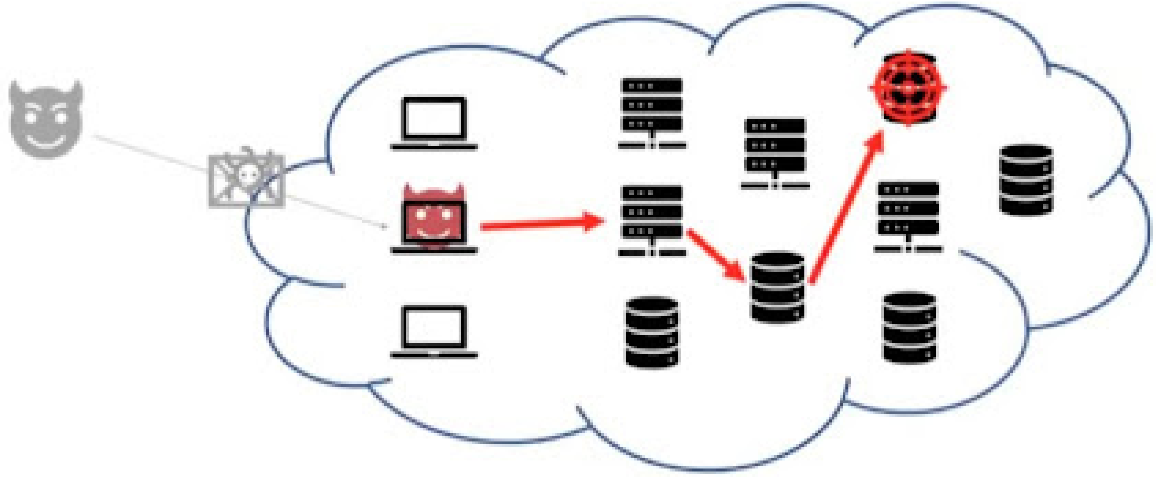


Figure 1: Lateral movement, depicted as red arrows, is the set of attacker movements between *internal* machines in an enterprise.

Let's Start a PIAs

- Remember PIAs will look different based on the questions you ask and orgizations
- Company supplied PIA are a good starting point
- We all have different networks and levels of risk we are willing to except.

Quick Review of some documents

- Company Supplied PIA
- Division PIA s

ThePhoto by PhotoAuthor is licensed under CCYYSA.

Scenario Rules

- **Use AI tools** to answer all questions.
- **Verify scenarios**: They involve actual companies and products.
- **Check official sources**: Visit company websites for accurate information.
- **Gather details proactively**: Do what’s necessary to find complete answers.

Answer the Following Questions for the Scenarios you have been provided

- What immediate questions do you have?
- Does this require a PIA – Yes or No, and why?
- If it requires a PIA, who should be on the PIA committee?
- What possible sensitive information could be at risk of exposure, and what are some ways you can manage it?
- What other polices or procedure might you have in your organization that might support or help mitigating the risk ?
- How do you find the answers to your questions?

- **Scenario 1**

A school has reached out because they are excited about purchasing a new **Huddle Camera** for their gym. The camera has advanced AI features and will be used to broadcast live sporting events. The school already pays for a Huddle subscription, and students and coaches actively use the software. They are now adding the camera and need it installed and connected to the network. They also mentioned that three other schools in the province are already using it.

- **Scenario 2**

Your HR department attended a conference and learned about an excellent program called **Workable**, an all-in-one HR software solution. They have already spoken with the sales representative. Workable has an outstanding security record, is **NIST compliant**, and will provide a completed **PIA**, so your organization will not need to complete one.

- **Scenario 3**

A local high school has been struggling with its automotive courses because the teacher hired has limited automotive experience. During community meetings, the school requested assistance, and the local automotive group offered to help. They plan to arrange for different automotive technicians to visit the school weekly throughout the semester to work with students and support the teacher in building confidence.

- **Scenario 4**

You are currently using **Education Forms** from Imagine Everything as a standalone product that integrates with your Student Information System, **PowerSchool**. The company has launched a new module called **Zenith**, which will handle online registration forms. They have promised to roll out several new features over the next two years to make the product more cost-effective. You previously completed a PIA for Education Forms, and the company has an exceptional reputation.

- **Scenario 5**

You receive an email from a teacher stating that **Canva** is free for students and educators. The teacher confirmed this with Canva, and Canva provided instructions for authenticating all school division accounts. Once set up, students and staff can log in with their school email and password for free access. The teacher requests that the IT department set up authentication because it will greatly benefit teachers and students, and not doing so could negatively impact learning.

- **Scenario 6**

Your purchasing department emails you after completing a 1.5-year RFI and RFP process. They have selected a new vendor for photocopiers and informed the vendor they are the successful candidate. It is now time to connect with the vendor’s IT department. The RFP included implementing **PaperCut** for secure printing, and the vendor also offers additional software that was part of the RFP conditions. The copiers and software are scheduled for installation over the summer, and since it’s only May, there should be enough time to finalize everything.

True and False PIA Questions (Review)

1. True/False: If another school division has already done a PIA on a specific product, you can just use theirs.
2. True/False: It is important for your tech team to be involved in every PIA.
3. True/False: If you cannot eliminate or manage all the risks in a PIA, you must not approve the product for use in your division.
4. True/False: Organizations after June 11/2026 must have a policy for completing PIAs.
5. True/False: Once you finish a PIA, it must be made available to the public.
6. True/False: Under the new privacy law, you must do a PIA for outside organizations that will provide services in your division.
7. True/False: Having a strong network and security setup helps with managing risks in a PIA.
8. True/False: Having clear consent policies (oral, electronic, and written) makes managing PIA risks easier.
9. True/False: If you already use a product or service, you do not need a PIA unless there is a major change.
10. True/False: PIAs are not needed if the software does not use or having any way of accessing personal information or school data.

SLQS Strand	How this presentation Supports The Strand
Building Effective Relationships	Collaboration, trust, transparency, stakeholder engagement
Modeling Commitment to Professional Learning	Ongoing learning, sharing research, critical reflection
Visionary Leadership	Innovation, future readiness, ethical practice
Leading Learning	Continuous improvement, data protection, professional development
First Nations, Métis, Inuit Education	Equity, cultural respect, privacy for all
School Authority Operations and Resources	Compliance, resource allocation, risk management
Supporting Effective Governance	Accountability, transparency, legal compliance
Workplace Wellness Framework	Safe environment, reduced stress, integrated professional learning

Contact: jesse.sadlowski@lethsd.ab.ca

Contact: jesse.sadlowski@lethsd.ab.ca