# Cyber Policies and Standards Why Now?

Andy Canty, Director of Cybersecurity Services

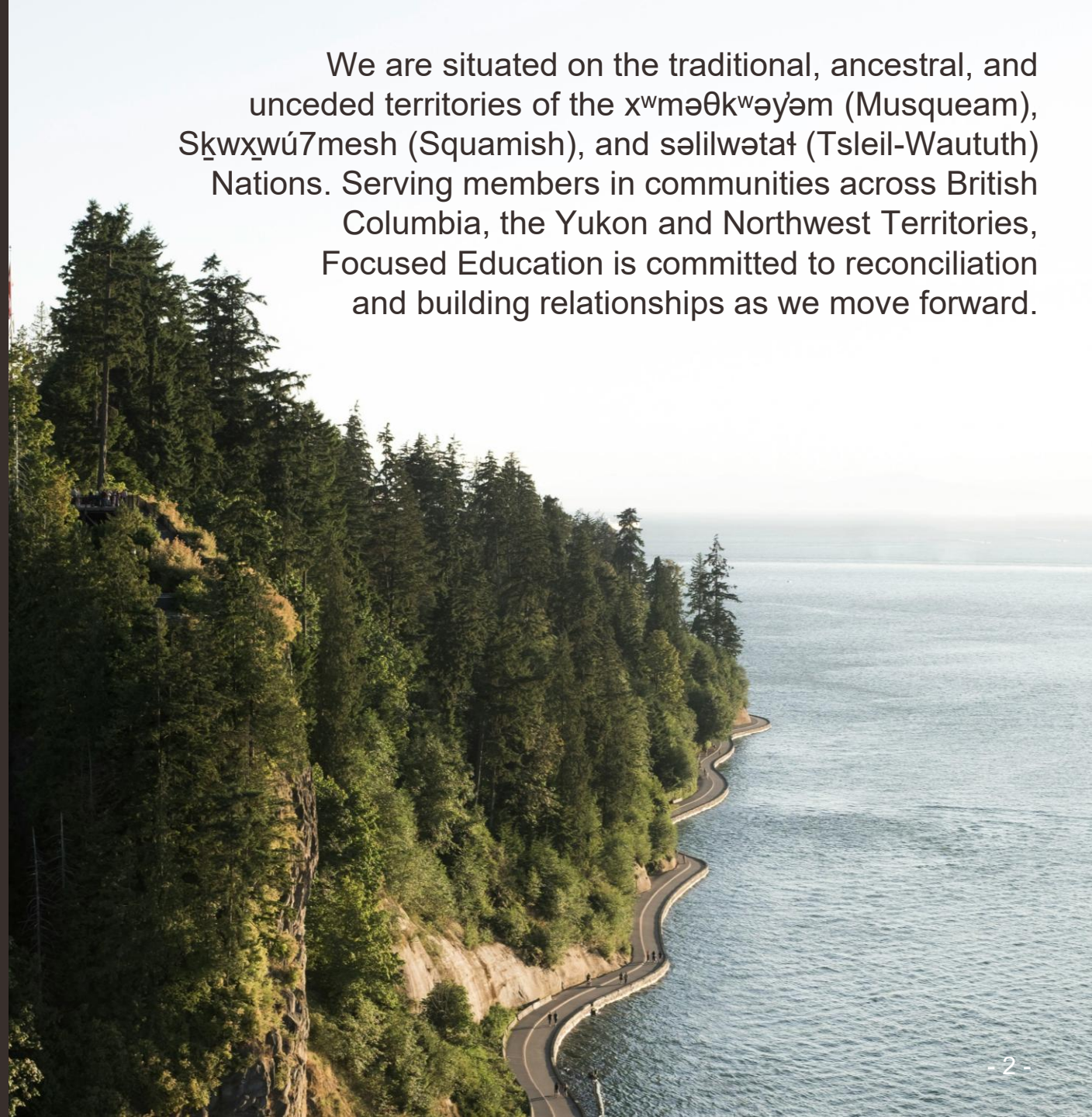
Working together to manage cybersecurity risk

FOCUSED EDUCATION RESOURCES

BUILDING CAPACITY. ADVANCING EDUCATION.

# Land Acknowledgement

We are situated on the traditional, ancestral, and unceded territories of the xʷməθkʷəy̓əm (Musqueam), Sḵwx̱wú7mesh (Squamish), and səlilwətaɬ (Tsleil-Waututh) Nations. Serving members in communities across British Columbia, the Yukon and Northwest Territories, Focused Education is committed to reconciliation and building relationships as we move forward.



FOCUSED
EDUCATION RESOURCES

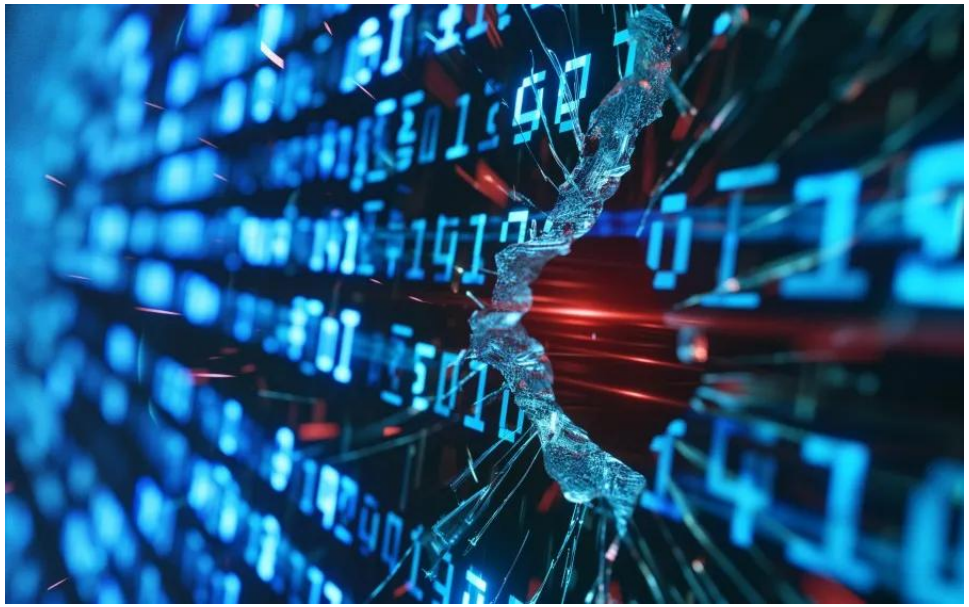
- Since the Policy Toolkit
- Revised Policy Template
- Acceptable Use Policy?
- The Policy Statements
- Q&A


FOCUSED
EDUCATION RESOURCES

# Since we published the Policy Toolkit

FOCUSED
EDUCATION RESOURCES

- Third party EDU vendor breach
- 5.2 million Canadians had their school records stolen
- Over 60m records in total
- $2.85 million ransom demand
- A ransom was paid
- Schools then extorted anyway



FOCUSED
EDUCATION RESOURCES

# What the regulators found

## IPC Ontario/Alberta OIPC

School boards “lacked policies and procedures to effectively monitor and oversee [the vendor’s] technical and security safeguards”

## Root cause

“An absence of security policies, not just a vendor failure.”

# Revised Policy Template

FOCUSED
EDUCATION RESOURCES

# Procedures without a policy

## The authority cascade. What breaks without the top tier

- **Policy** (board-approved) - sets the authority, accountability, risk appetite.
- **Standards** (management-maintained) - define control objectives/metrics.
- **Procedures** (staff-maintained) - how controls are implemented.

Without the policy layer, the layers below have no governance anchor.

Best guesses that cannot serve as evidence of due diligence.

# Information Security Policy

## Principles based policy template for K-12

- 1 board document
- 14 policy statements
- 13 staff documents
- 7 pages
- 1 board vote


FOCUSED
EDUCATION RESOURCES


# AUP?

FOCUSED
EDUCATION RESOURCES

# More than Acceptable Use Policy

1. Protects as a governance obligation, not an IT task
2. Protects from *unauthorized* access - external
3. Ensures continuity of learning and operations
4. Creates a paper trail
5. Embeds CIS, NIST or other frameworks as the control architecture

*“If we were investigated tomorrow, what policy would we point to?”*

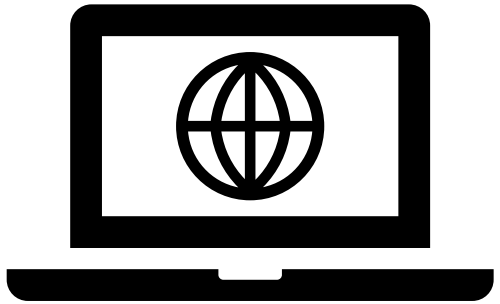
# The policy statements and why they matter

## 1. Governance and Risk Management

- Cybersecurity risk is enterprise risk
- Has the Board consented to carry the risk?
- Framework
- Authority
- Accountability

## 2. Asset Management

- All the things! K-12 is a little crazy with assets
- Discover asset gaps at the worst time
- Shadow IT is a procurement issue first
- Asserting compliance we cannot demonstrate
- “What systems were affected?”



## 3. Audit and Review

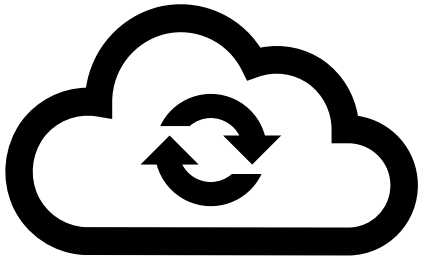
- Are the controls effective?
- No convincing needed for this one…

## 4. Backup and Retention

- Ransomware is a recovery problem
- Ransoms get paid because recovery not viable
- Over retention multiplies the breach radius

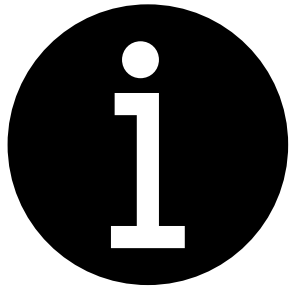
## 5. Cloud Security

- ‘Reasonable security’ regardless of where stored
- Every app used is an agreement you are responsible for
- Uncontrolled spend and unmonitored data exposure
- Line dividing district and vendor needs contract



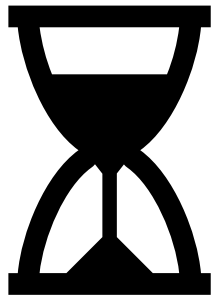
## 6. Data Protection

- Privacy, cyber & AI all increase requirement
- K-12 culture not best fit for least access
- Increases the need for policy and process
- Cannot protect everything equally
- Ringfence before full classification



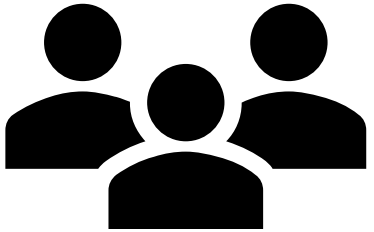
## 7. Disaster Recovery and Business Continuity

- RTO (Recovery Time Objective): How long is too long?
- RPO (Recovery Point Objective): How much data loss?
- Hardware failure: random, data intact, repair possible
- Ransomware: intentional, data stolen, evolving



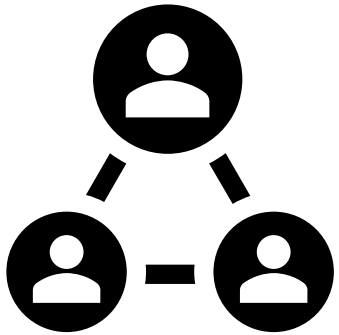
## 8. Human Resource Security

- Staff awareness training is high value, just like MFA
- AI phishing is getting good
- Contractor signature required for legal obligation



## 9. Identity and Access Management

- Single compromised account + no MFA = 60m records
- Slow down – add extra gates for privileged access
- Internal audits (Entra ID Assessment high risk findings)
- Dormant accounts are high risk but no value



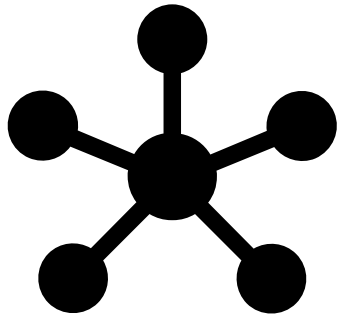
## 10. Incident Management

- Think of it like CIRT (student/staff safety)
- Find the gaps before the attackers
- The biggest challenge is the ST's schedule!

FOCUSED
EDUCATION RESOURCES

## 11. Network Security

- Significant work involved
- But attackers don’t land straight on the target
- They navigate the insecure (flat) network
- Focused ED scoping plan to assist



## 12. Physical Security

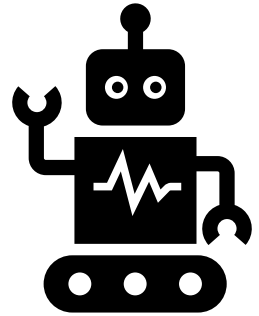
- Well understood domain
- Just needs to be documented and tested

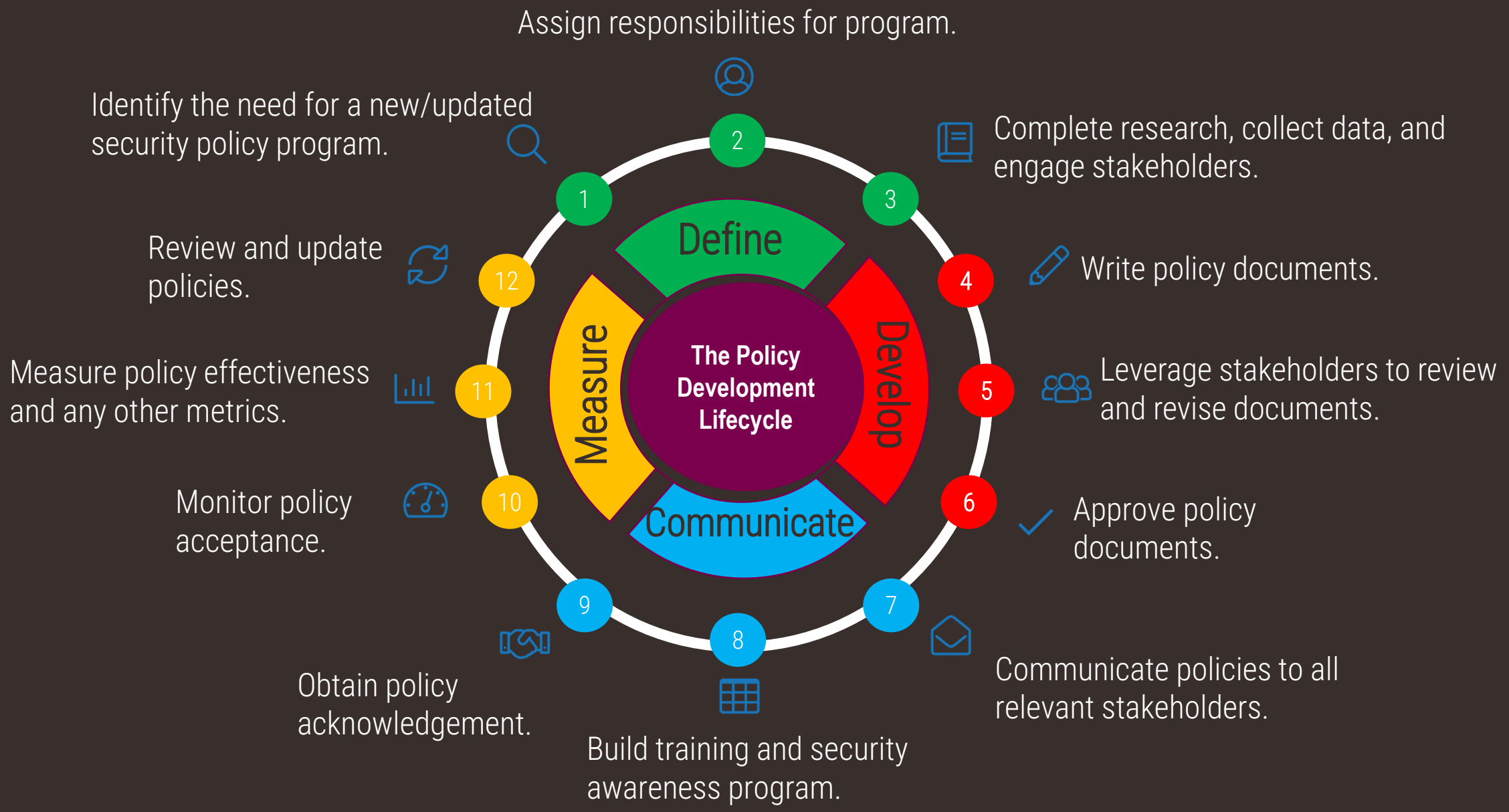
## 13. Vendor and Third-Party Management

- FIPPA obligations travel with the data
- New contract language required:
  - Encryption
  - Breach notification timelines
  - Subcontractor restrictions
  - Audit rights
  - Certifications

## 14. AI Security

- That copy and paste into AI :
  - Appears on no software asset inventory
  - Is covered by no contract
  - Processes data you are legally responsible for
  - Before anyone knows the tool exists
- AI Security is a subset of AI Governance






InfoTech Research. Diagram inspired by: ComplianceBridge, 2021

Thank you for your time

Any questions?