New Governance Documents: An overview

Governance and Policy Working Group
Fall 2022

Agenda

- Why are we here
- Document Hierarchy and Development Process
- Implementation of Policies and Standards
- Overview of Approved Policies, Standards, and associated documents
- What’s Next: Policies and Standards in the pipeline.
- Reminders and next steps

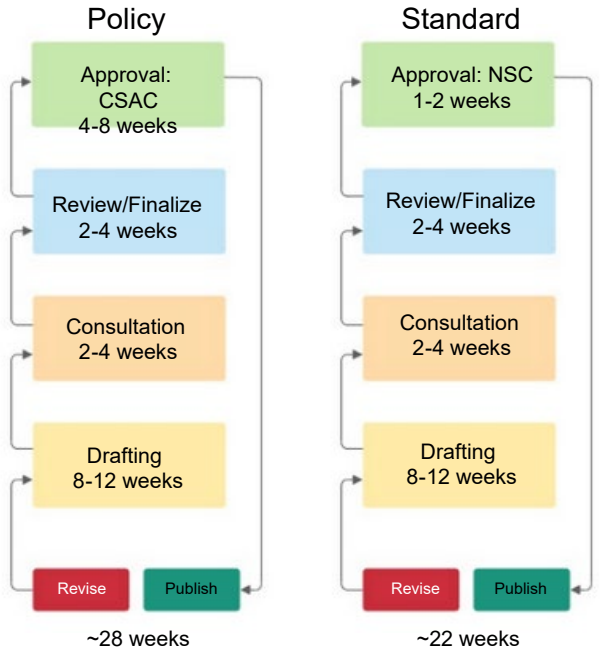
Why are we here?

- To show how documents are created and where the approved documents are published
- The security program must include communication and awareness in order to be effective
- Facilitate a common set of expectations for everyone including users, including process and technical controls
    - These policies will affect you and your work and you need to be aware of key points
- We haven’t done a S2S in awhile

Document Hierarchy Map

How Governance Documents are developed

- Subject WG or Policy WG (with external SMEs)
- Review by NSC & Community prior to approval
- Approval: CSAC for policies, NSC for standards
- Change and feedback logs maintained



Implementation of Policies and Standards

- You can start today! (e.g. new projects and services)
- The framework assumes all National Services will comply with these requirements
- Some Policies and Standards will take time to implement (expectations noted for each) and specific implementation efforts will proceed in the fullness of time

SEC-00 Glossary of Terms

Status: Approved and In Force

- The source of truth for definitions
- Will change frequently as other Policies and Standards are developed
- Definitions are difficult and important
- Avoided re-defining industry standard “dictionary” terms
- Avoid defining a term with one meaning to mean something else

SEC-02 Data Classification Policy

Status: Approved and In Force

- Four levels of classification based on relative importance or sensitivity
- Examples given for each classification are not exhaustive
- Data Owner can classify higher but not lower
- Classification allows us to know how to treat classes of data differently
- Data Owners will *tell us* their classification so we know how to treat it

SEC-03 Data Handling Standard

Status: Approved and In Force- 1 year transition period

- Includes placeholder information for Policies and Standards that do not yet exist.
- Therefore some sections are more general where others (eg Transmission of Data) are more detailed.
- Will be linked to other documents as they become available and this document will change

SEC-05 Cybersecurity Risk Management Policy

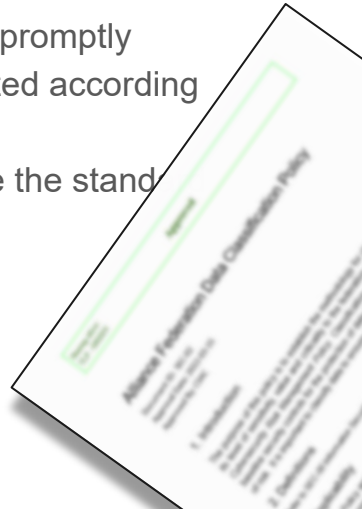
Status: Approved- Implementation in Progress

- Standardizes Identification of Risk and Appetite for Treatment - Including Documentation (Register)
- Ultimately will help improve Cybersecurity Posture
- Risk Assessment Project starting- NSC will be contacting SMEs to kickoff project
- (Risk Assessment Procedure is available)

SEC-04 Vulnerability Management standard

Status: Approved and InForce, 1 year transition period

- Vulnerability lifecycle: scanning -> results handling-> remediation -> reporting
- Higher severity vulnerabilities generally pose greater risk and need to be dealt more promptly
- Untreated vulnerabilities pose risk to the organization, and risks should be documented according to risk management policy
- Key items like OSAC and Risk Register don’t exist yet and need to be defined before the stand can come into play



Policies and Standards in the pipeline

- Cybersecurity Policy
- System Logging and Security Monitoring Standard
- Asset Management Standard

Reminders and next steps

- All policies and standards will be here https://alliancecan.ca/en/policies
- Alliance Federation HQP are expected to familiarize themselves with these documents
- We suggest users do the same.
- Feedback is always welcome email: security@tech.alliancecan.ca