

**FRCOG IT / Cybersecurity Workshops – NOVUS Insight  
Fall 2021**

## **Workshop 1: Positioning Technology & Cybersecurity as a Strategic Imperative**

**Target Audience: Executive Leadership, Selectboard Members**

### **Session 1 - Support and Planning**

Tuesday, September 14, 2021. 9am-10:30am.

**Registration link:** <https://us02web.zoom.us/meeting/register/tZEuc-yorDIqGd2rIbDdsXRh1QyK0DX-Q-dw>

- Myth-busting – “Tech is overhead.” No, it’s not.
- Why secure technology is the foundation of modern government services
- Solving the budget problem starts with cultivating buy-in
  - How to talk tech without talking tech
  - How to (more) confidently sell stakeholders and constituents on the need for tech & cyber budgeting
- Creating strategic plans that are supported by technology

### **Session 2 - Internal Change Management**

Thursday, September 30, 2021. 1pm-2:30pm.

**Registration link:** <https://us02web.zoom.us/meeting/register/tZMsceryqD0pG9UpZvNaUA67TvUL4ral-CSp>

- Breaking old habits - creating a culture to support change
- Incorporating policy & procedure development and incident response planning into municipal budgets
- Creating more of a culture of cybersecurity

## **Workshop 2: Best Practices in IT/Cybersecurity Policies and Procedures Workshop**

**Target Audience: Executive Leadership, IT Personnel**

### **Session 1 - Overview of a Cybersecurity Program**

Thursday, October 14<sup>th</sup>, 2021. 9am-10:30am.

**Registration link:** <https://us02web.zoom.us/meeting/register/tZEtdcupzqkvEtRlOUogvLkP1cgKJkRm-132>

- Understanding the important distinctions and interrelationship between policies, procedures, guidelines, and standards
- Relevance -- How does my cybersecurity program relate to and impact the day-to-day operations of the municipality?
- Components of a cybersecurity program and the importance of each

### **Session 2 - Building a Cybersecurity Program**

Tuesday, October 26<sup>th</sup>, 1pm-2:30pm

**Registration link:** <https://us02web.zoom.us/meeting/register/tZMtdOqsri8tE9Y93xSt58Ks1W9lBXdqu838>

- Templates that will get you started
  - Using the templates to drive other components of your overall IT program such as backup and recovery, incident response, and IT asset management
- The role of executive leadership
- Regulatory requirements
- Making the program understandable and relevant to all -- employees, board and commission members, external parties, the public

**FRCOG IT / Cybersecurity Workshops – NOVUS Insight  
Fall 2021**

### **Workshop 3: Incident Response Planning Workshop**

**Target Audience: Executive Leadership, IT Personnel, Emergency Operations & Critical Infrastructure (i.e. WPC)**

#### **Session 1 – Introduction of the cyber incident response plan template and implementation checklist tool**

Wednesday, November 3, 2021. 9am-10:30am.

**Registration link:** [https://us02web.zoom.us/meeting/register/tZMtDumuDorGd3etwF0WULXvyexlcPKZVsm](https://us02web.zoom.us/join/https://us02web.zoom.us/meeting/register/tZMtDumuDorGd3etwF0WULXvyexlcPKZVsm)

- Identifying and understanding the municipality's key information assets and the risk of them being breached or removed
  - Novus will provide an asset inventory worksheet for collecting and categorizing assets
- Identifying whether assets are within your control or a third party's, or if it is a shared responsibility
- Understanding your in-house capabilities vs. need for external expertise/resources
- How to assemble an incident response team

#### **Session 2 – Implementing an IRP and addressing tool implementation barriers and /questions**

Wednesday, November 17, 2021. 1pm-2:30pm

**Registration link:** [https://us02web.zoom.us/meeting/register/tZUuceyuqzkqGtU7cUa077aUdvR6pwj69Tk3](https://us02web.zoom.us/join/https://us02web.zoom.us/meeting/register/tZUuceyuqzkqGtU7cUa077aUdvR6pwj69Tk3)

- Preparing a tailored Incident Response Plan including:
    - Guidelines for who to inform when data is breached or exposed
    - Establishing the severity of a breach and the level of response required
  - How your IRP should fit within your business continuity and disaster recovery strategies
  - How to test your incident response plan
- \* Each participant will leave with a set of materials and templates allowing them to custom tailor their plan.**

### **Workshop 4: Security and Compliance Workshop**

**Target Audience: Executive Leadership, Any departments dealing with sensitive information (i.e. Police, Fire, HR)**

Thursday, December 2, 2021. 9am-11am.

**Registration link:** [https://us02web.zoom.us/meeting/register/tZUoc-iuqT0pGd34UEJtny2hUh2UqetDuVsd](https://us02web.zoom.us/join/https://us02web.zoom.us/meeting/register/tZUoc-iuqT0pGd34UEJtny2hUh2UqetDuVsd)

- Most common sensitive data types in a municipality
  - PII
  - PHI (the 2 things needed with data for it to be considered PHI and regulated by HIPAA)
  - FERPA
  - CJIS
  - PCI
- Identifying sensitive data in your environment
- Strategies for protecting sensitive data and end user education
- When all else fails, there's insurance. An overview of cyber insurance and what's included.
- FOIA, record retention, and e-discovery
- Baseline standards and best practices for a security and compliance program

### **Workshop 5: State IT/Cybersecurity Efforts and Resources Workshop**

**Target Audience: Executive Leadership, IT Personnel**

Thursday, December 16, 2021. 9am-10:30am.

**Registration link:** [https://us02web.zoom.us/meeting/register/tZMtcOqurD0rG9wtjXL5oJ7Isbxh2cbQtfsA](https://us02web.zoom.us/join/https://us02web.zoom.us/meeting/register/tZMtcOqurD0rG9wtjXL5oJ7Isbxh2cbQtfsA)

- Overview of Massachusetts-specific municipal IT and security resources
- Presentations by representatives from state agencies, MIIA, and potentially federal resources