TUNING THE INCIDENT RESPONSE PLAN

Use this checklist to help customize the Incident Response Plan to ensure that it works optimally for your municipality.

BEFORE YOU BEGIN

- ☐ Watch the online training video that support this plan using this link HERE.
- ☐ Read and implement the Incident Response Plan and this checklist. Find on JIF website HERE.

COVER PAGE

- ☐ Change the logo and document title to uniquely identify it as your municipality.

DOCUMENT MANAGEMENT TABLE

- ☐ Adjust this table to align it with the approach you use to manage other documents.
- ☐ Update the table with your information. The most important fields are Version, Owner, and Next Review. The plan should be reviewed at least annually.
- ☐ Put a copy of your policy in the "Cloud" so that if your IT infrastructure or offices aren't available, the policy remains accessible.

POLICY STATEMENT (SECTION 1)

- ☐ The policy statement communicates the policy's purpose. We kept this very simple. You can expand upon it if there is something specific you think is critical to communicate.

REASON FOR THE POLICY (SECTION 2)

- ☐ If you have a more complex municipality (e.g., run a shared services model or operate a Utility Department) you may potentially want to enhance this statement to ensure that the reader understands the increased level of risk for your model (e.g., an incident may impact public safety).
- ☐ If so, emphasize that an effective Incident Response may minimize that specific impact. This reinforces the importance of the policy.

SCOPE (SECTION 3)

- ☐ Consider whether your municipality's unique services and exposures might influence the incident types that you should list.
- ☐ Appoint an Incident Response Manager and ensure that they are part of your training process.
- ☐ Establish an Incident Response Team.
- ☐ Determine how to best communicate incident reporting responsibilities to all employees. Ensure that those mechanisms are as simple as possible to use (e.g., phone call).

INCIDENT RESPONSE PHASES (SECTION 4)

- ☐ Update the list of people that the Incident Response Manager is responsible to contact.
- ☐ Have the Incident Response Manager decide on: "Procedures to isolate the computer from the network OR unplug it from its power source." (Section 4.1)
- ☐ Ensure that the Incident Response Roadmap is up to date and clearly understood by all responsible parties.
- ☐ Consider adding guidance to Sections 4.3 & 4.4 that is specific to your municipality's operations.

☐ Ensure that the Incident Response Team table is fully populated with anyone that will need to be contacted or consulted with during an incident.

SPECIAL SITUATIONS/EXCEPTIONS (SECTION 6)

☐ If you are a "Bring Your Own Device" (BYOD) shop in any way, this is an important clause to include. Even if you aren't, it's good "insurance" in case someone is using a personal device on your network or works from home.

RELATED INFORMATION (SECTION 7)

☐ Please add any other relevant information pertinent to your municipality. Remember to adhere to the standards described in the MEL Technology Proficiency Program to keep your municipality safe from cyber attacks.

DEFINITIONS RELATED TO CYBER LIABILITY INSURANCE (SECTION 8)

☐ Ensure that the Incident Response Manager understands the criterion tied to choosing Step 5 or Step 6 in Section 4.1. Example: Is the event a cyber breach or low level incident? If unsure, please always report by following the Cyber Incident Claim Roadmap instructions.

IN CONCLUSION

☐ Contact your JIF Fund Professionals with any questions you may have.
Paul Forlenza: Paul_Forlenza@ajg.com | 856-446-9135
Paul Miola: Paul_Miola@ajg.com | 856-446-9130

☐ Ensure that the Incident Response Plan has been communicated to all Incident Response Team Members as well as municipal employees and that their responsibilities are well understood.

☐ Ensure that employees know how and when to report a potential incident.

☐ Ensure that the Plan is stored in a secure and highly available location and that all Incident Response Team Members and employees are advised of the location.

☐ Consider scheduling an Incident Response exercise to ensure the plan works as intended.

☐ Mark your calendar for one year from today to review/update the plan.