

Cybersecurity Checklist

1 Do you have an Incident Response Plan/Disaster Recovery Plan?

Yes No

 **Have you exercised the Plan?**

Yes No

 **Do you have an “out of band” communications plan?**

Yes No

2 Who is your Internet Provider?

3 Do you have Cyber Insurance?

 **What does it cover?**

 **Are there required actions to be taken to keep it in effect?**


4 Do you have a backup system in place?

Yes No

 **How far back do backups go?**

 **Is your backup system on Windows or Linux based?**

- **If it is Windows based, is it domain joined?**
- **Does it have a firewall on it and malware protection?**

 **How is your backup system connected to the network (ie same layer 2 or layer 3 segment as your other systems)?**

5 Do you have an IDS/IPS?

Yes No

 **If yes, it is in monitoring or blocking mode?**

6 Do you maintain/review logs?

Yes No

 **Are logs kept offline?**

Yes No

7 Network topology diagram (up-to-date)

8 Complete asset list (servers, PCs, backups, etc)

A Network Diagram

- 1 Verify the diagram so it is understood**
- 2 If a diagram does not exist one needs to be created**

B IP Scheme

- 1 Management Network**
- 2 Phones**
- 3 Servers**
- 4 Workstation**
- 5 Wi-Fi**

C List of Assets Building #1 (Repeat as necessary to list all sites)

1 Routers

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

2 Switches

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

3 Phone System

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

4 Servers

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

5 Workstations

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

6 Video Surveillance System

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

7 Networked Door Badging System

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

8 Networked Alarm System

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

8 Other Systems

- A Number of Devices**
- B Make**
- C Model**
- D Operating System**
- E Firmware Version**

9 Software/applications list

10 Define critical assets with prioritization levels for recovery

11 Define critical information with prioritization levels for recovery

12 Identify patient zero and preserve in as-is form

13 Where is your payroll info?

 **Can you pay employees with the network down?**

Yes No

14 Is the 911 System affected if network is down?

Yes No

 **Is CAD data affected?**

Yes No

 **Do you have a 911 COOP Plan?**

Yes No

15 Do you maintain CJIS data?

Yes No

16 Do you maintain DHHS data?

Yes No

17 Is email affected by network outage, or do you have a cloud-based system?

18 Can you provide student meals when network is down (K-12)?

Yes No

19 If your phones are VOIP, are they on a separate VLAN?

Yes No

20 Is the alarm system effected by a network outage?

Yes No

21 Do you have trusted connections with other Agencies?

Yes No

Please identify agencies with whom your agency shares a trusted connection.

22 Do you know who your local Emergency Manager is?

23 Do you have a listing of Names and phone numbers of key contacts?

- 1** Chief Executive Officer (CEO)
- 2** Chief Operations Officer (COO)
- 3** Chief Financial Officer (CFO)
- 4** Chief Administrative Officer (CAO)
- 5** Chief Technical Officer (CTO)
- 6** IT Manager
- 7** Network Administrator
- 8** Key Staff
- 9** Others