



# MONTGOMERY COUNTY CYBER INCIDENT RESPONSE PLAN

OFFICE OF EMERGENCY MANAGEMENT AND HOMELAND SECURITY

# CYBER INCIDENT RESPONSE FRAMEWORK

- April 2017
  - Contract support
  - 1<sup>st</sup> round of meetings with key stakeholders
- Background and Purpose
  - Recognizing that a cyber incident could require the coordinated response from multiple county government agencies, the Montgomery County Office of Emergency Management and Homeland Security (OEMHS) set out to create a Cyber Incident Response Plan (the “Plan”) which will clearly outline the county’s response to a cyber incident affecting county government.
  - This Plan will supplement the existing response plans that the county’s Department of Technology Services (DTS) has already developed and implements.
    - DTS plans focus on the technical aspects of any cyber incident, outlining the steps DTS takes in responding to such incidents. The OEMHS Cyber Incident Response Plan will focus on non-technical aspects of a county response to a cyber incident.
  - The Cyber Incident Response Plan will conclude by establishing a training and exercise program to ensure the periodic testing of the Plan and to provide opportunities for improving the Plan.

# SCOPE

The Office of Emergency Management and Homeland Security (OEMHS) may be called to coordinate the response to a cyber incident when:

1. There is an attack or impending attack on County assets in which public services and/or government operations are impacted. In this case, DTS will be the lead agency responsible for responding and remediating the threat/ attack.
2. There is an attack on non-county assets, which impact County citizens and critical infrastructure or services. In this case, DTS will not be the lead in the response and remediation efforts, however will serve as a SME for cybersecurity. OEMHS will coordinate the response to the event in accordance with the County's EOP though an all hazard approach. DTS may be responsible for remediating County portions of systems that may be impacted by the external disruption.
3. Delineate roles and responsibilities for holistic cybersecurity posture for the county from strategy and policy, operations, and tactical support.

# DEFINITIONS

- **A security incident** is defined as any event that threatens the security of the County's information technology resources. This includes a violation or imminent threat of violation of the County's Security Administrative Policy (AP), Security Policy, System Security Plans(SSPs), security laws and regulations such as HIPAA, CJIS Security Policy, contracts such as PCI, other inter-connect agreements between the County and outside entities, and any other adverse event that compromises the confidentiality, integrity, and availability (CIA) of the County's information technology enterprise.
- **A security incident response** involves the efficient and effective deployment of all available and appropriate resources in response to a reported security incident. Incident response policy and procedure creation is also an integral part of establishing a Computer Incident Response Team(CIRT,) so that incident response is coordinated and performed effectively, efficiently, and consistently.



# LEVELS OF INCIDENT



Level	DTS Description	Supplemental Emergency Management Definition
<b>Level 0 [non-incident]</b>	this would comprise of incidents that may potentially be classified as a Level 1 incident based on the minimal impact on CIA confidentiality, integrity, and availability; policy violation, and/or business operation. But after further investigation, CIRT may determine that it did not merit Severity Level 1 to be considered a security incident.	Unsubstantiated or inconsequential event.
<b>Level 1 [low]</b>	this would comprise of routine incidents. Typically, an incident in this category would have little or no impact on business operations, information disruption or disclosure, or technical policy violation.	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
<b>Level 2 [med]</b>	an incident within this category will cause minimal disruption to business operations, disclosure of critical data and/or a violation of security policy. Usually, this would require little effort to achieve containment and recovery for incidents at this level.	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
<b>Level 3 [high]</b>	the impact of an incident in this category will be significant. This will cause major business disruption or disclosure and/or a security policy violation.	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
<b>Level 4 [critical]</b>	an incident in this category will have major impact on business operations, policy and/or legal violation, as well as some risk of negative financial implications and public relations impact. This typically demands public disclosure and the involvement of an external agency or department, such as the FBI and News media.	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties
<b>Level 5 [most critical]</b>	this is the highest level of severity and constitutes any incident that could potentially jeopardize human life or reputation, criminal activity that violates Federal, State, or Local laws, significant risk of financial loss or public relations impact.	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or to the lives of US persons.

# ROLES AND RESPONSIBILITIES

<b>Strategy and Policy</b>	County Council Director of Office of Emergency Management and Homeland Security CISO Information Technology Policy Advisory Committee Security Committee Technical Operational Management Group
<b>Operations</b>	CISO CIRT Director OEMHS
<b>Tactical Support</b>	Tactical Support





# NOTIFICATIONS ABOUT CYBER INCIDENTS

- Incident Level
  - Agencies Involved
  - Internal vs. External Communications
- 
- 



# COORDINATION OF CYBER INCIDENT RESPONSE

- Normal Operations
  - Enhanced Monitoring
  - Partial Activation
  - Full Activation
  - Increasing and Decreasing Phases
- 
- 



# STATE AND FEDERAL COORDINATION



- State
  - MEMA
  - DoIT
  - MCAC
- Federal

# ROLE OF COUNTY WHEN PRIVATE SECTOR AFFECTED

- OEMHS: consequence management
- Office of Public Information: communication
- Police: investigation
- All other agencies: as needed
- State and Federal agencies



# OTHER CONSIDERATIONS

- Post-incident
  - Training and exercise
  - Plan maintenance
- 
- 

An abstract graphic on the left side of the slide, consisting of a network of thin, light-blue lines and small circles, resembling a circuit board or a neural network diagram. The lines and nodes are concentrated on the left edge and spread out towards the center.

QUESTIONS?