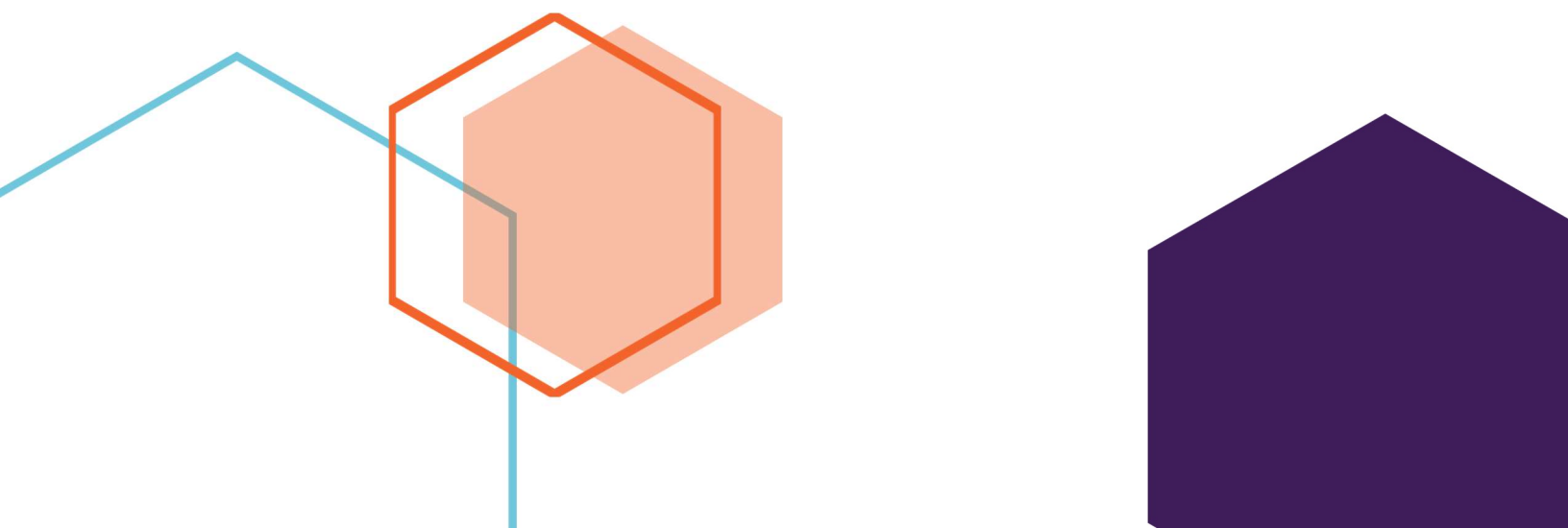




LOCALITY ENGAGEMENT GUIDE

Locality Guide to Cyber Incident Response

The Locality Guide to Cyber Incident Response provides city and county leaders with an overview of the Commonwealth's capabilities in response to reported cyber incidents, as well as other helpful cybersecurity resources.





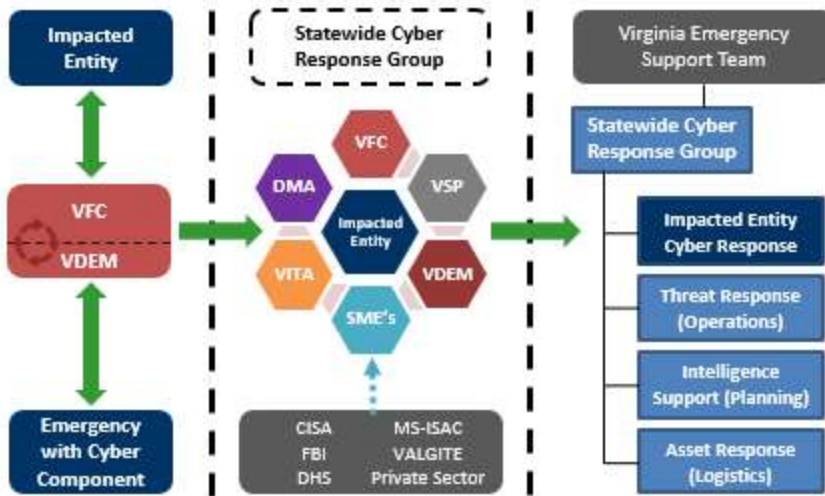
LOCALITY ENGAGEMENT GUIDE

Locality Guide to Cyber Incident Response

The Strategy

Virginia's cybersecurity strategy includes a "Whole-of-Commonwealth" approach to ensure a more secure and resilient Virginia. This includes the ability to surge resources from local, state, federal, and other outside partners in response to a reported cyber incident, reducing the number of individual agencies that need to be contacted while delivering a more holistic and effective response. The impacted entity remains at the center of the response process as a key decision maker.

The Process



Available Services

The level of support provided scales significantly based on the incident, from intelligence analysis and basic advisory services all the way to integration with the Virginia Emergency Support Team (VEST) for significant events or emergency declarations resulting from or relating to cybersecurity incidents. The Virginia National Guard or Virginia Defense Force may also be detailed to provide variable levels of assistance depending on the nature of the incident.

Reporting an Incident



The Virginia Fusion Center (VFC) acts as the primary hub for incident reporting. Incidents can be reported to vfc@vsp.virginia.gov or 804-674-2196.

Based on the severity and potential impact, partners from multiple agencies are tasked to provide support for the impacted entity, with a focus on returning to "steady state" as quickly and safely as possible.

Significant cyber incidents potentially impacting public health or safety, critical infrastructure, or community lifelines may receive further support from VDEM.



DATA SECURITY & INFORMATION SHARING

The Virginia Fusion Center (VFC) maintains an intelligence management database that is used to store information received. The VFC complies with all cyber security requirements put forth by the Commonwealth of Virginia and published by the Virginia Information Technologies Agency (VITA). The VFC monitors for any necessary adjustments to ensure continued compliance with these security requirements.

VFC personnel are subjected to a comprehensive lifestyle background investigation and are required to maintain a secret-level security clearance issued by the U.S. Department of Homeland Security (DHS).

Information possessed by the VFC is exempt from Freedom of Information Act requests and is protected from unauthorized dissemination by Code of Virginia [§ 52-48](#) and [§ 52-49](#), as well as [§ 2.2-3705.2](#). Prior to sharing any intelligence received the VFC shall notify the data owner and remove any identifying information making it non-attributable.





The sharing of cyber intelligence follows standard procedures such as the Traffic Light Protocol (TLP). The following information is provided by the Cybersecurity Infrastructure Security Agency (CISA) for understanding the handling of TLP information. "TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s)."

Localities are the caretakers of the data entrusted to them by the citizens and the information used by agencies to perform their local government functions. The agencies and departments called upon to respond to a request for assistance in planning for, preventing, responding to, and/or mitigating a cyber incident are respectful of this responsibility and confirm the locality's ownership of their data. As such, the locality is responsible for deciding what is to be done with any data shared with the agencies and departments. Any storage of such data will be the responsibility of the owning locality.

Some services or capabilities available from state, federal, or other outside partners may require the signing of, or agreement to, certain non-disclosure agreements (NDA's) or memorandums of understanding (MOU's). These are typically handled at the onset of an incident or service delivery when identified as a requirement for continued support.

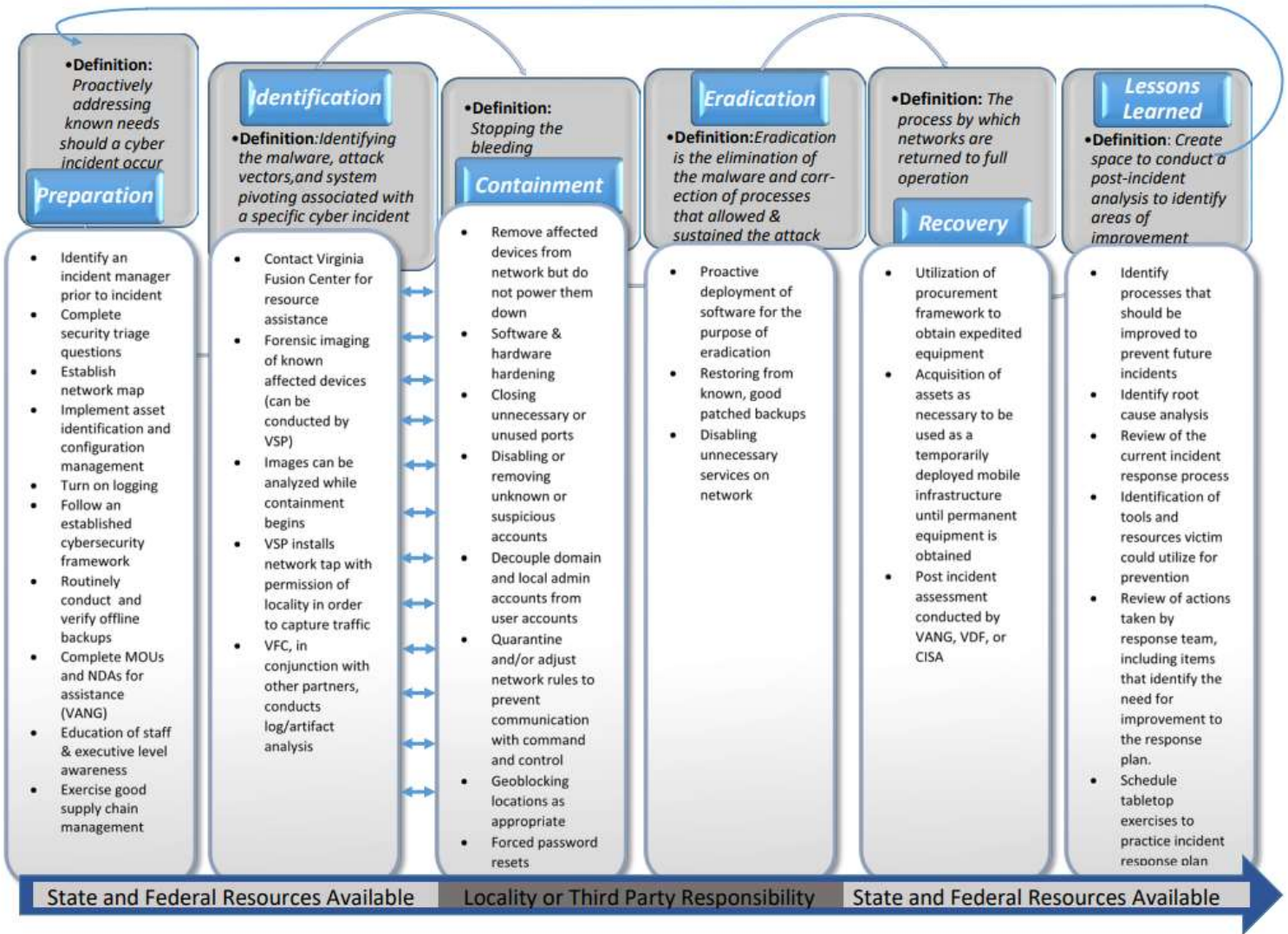
LOCALITY ENGAGEMENT GUIDE



Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>



INCIDENT HANDLING PROCESS



The Commonwealth of Virginia relies on a number of standard models and frameworks to guide and inform the incident response process. Chief amongst these are the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), as well as the NIST Special Publication 800-61 Rev. 2 - Computer Security Incident Handling Guide.

The impacted entity remains at the center of the response process as both a key member of the response effort and key decision maker. Significant cyber incidents may also undergo a formal after action report (AAR) process to derive appropriate lessons learned with a variety of stakeholders and better inform future response efforts.



INCIDENT LIFECYCLE & ENGAGEMENT CHECKLIST

PRE-INCIDENT ENGAGEMENT CHECKLIST

- Identify a locality incident manager. This will aid in a more organized approach in the event of any cyber incident.
- Confer with management, cyber insurance provider, and legal counsel to identify overall response process prior to incident.
- Develop a plan for public notification in the event of a successful data breach in partnership with your cybersecurity insurance provider.
- Review list of available resources (see Additional Resources).
- Review the [Fusion Center Cyber Incident Intake Form](#) for the types of information that will be requested during an incident.
- Maintain at least 30 days of logs on systems whenever possible to enable a more effective response.
- Establish a routine process for local and offline backups and test them regularly to enable a more effective recovery.
- Complete or establish any necessary memorandums of understanding (MOUs) and non-disclosure agreements (NDAs) prior to an incident.

ACTIVE INCIDENT RESPONSE CHECKLIST

- Notify your cybersecurity insurance provider.
- Request assistance from State and Federal cyber partners: Contact VFC at 804-674-2196 or vmc@vfc.vsp.virginia.gov.
- Be prepared to provide as much information as possible (see [Fusion Center Cyber Incident Intake Form](#)).
- Additional actions you may wish to take to contain the incident:
 - Remove or isolate affected devices from network connections, but **do not** power down.
 - Identify/close unnecessary or unused ports and processes.
 - Disable or remove unknown or suspicious accounts.
 - Decouple domain and local admin credentials from user accounts.
 - Implement rules to prevent communication with malicious IP's or domains, including geo-blocking locations as appropriate.
 - Force password resets on potentially impacted accounts.
- Only restore from known "good" backups.

Key Contacts



Virginia Fusion Center
vmc@vsp.virginia.gov
 or 804-674-2196.

The MS-ISAC Security Operations Center is available 24/7.
soc@msisac.org
 or 866-787-4722

DHS CISA
central@cisa.dhs.gov
 888-282-0870

FBI - Internet Crime Complaint Center
[Submit a complaint](#)
 804-261-1044

Virginia Office of the Attorney General – Computer Crimes
oag.state.va.us
 804-786-2071



POST-INCIDENT RESPONSE CHECKLIST

- Schedule and conduct an after action review of the entire incident response process.
 - Conduct a root cause analysis to fully explore everything that contributed to the incident.
 - Review existing policies, processes, and procedures to identify areas for change or improvement to better prevent or mitigate similar incidents in the future.
 - Discuss the decisions made and actions taken by leaders and response team members to help drive useful discussions.
 - Create a short-term and/or long-term plan to address the recommended changes or fixes identified in the after action review, and monitor progress towards implementation.
- Establish continuous monitoring capabilities if not already present, and/or monitor logs for anomalous activity for at least 30 days after incident.
- Schedule and conduct a post-incident vulnerability assessment to ensure security risks or other identified gaps have been mitigated.
- Identify tools, services, or other resources that can be used to address security risks or gaps you otherwise could not fix or mitigate.

ADDITIONAL RESOURCES

*See the more extensive list of services for detailed information (titled CIU Resources.xlsx)

Phase	Resource	Provider*	Cost	Contact	Requirement
Preparation	Security Assessments	VANG/VDF	Free	WebEOC request through local emergency manager	Signed MOA/NDA
Preparation	Cyber Intelligence Products	VFC	Free	vfc@vfc.vsp.virginia.gov	Signed NDA
Preparation	Virginia Cyber SHIELD	HSIN/VFC	Free	vfc@vfc.vsp.virginia.gov	HSIN account
Preparation	Cyber Resilience Review (CRR)	CISA	Free	Central@cisa.dhs.gov	None
Preparation	Vulnerability Scanning/Cyber Hygiene (CyHy)	CISA	Free	Central@cisa.dhs.gov	None
Preparation	Phishing Campaign Assessment (PCA)	CISA	Free	Vulnerability@cisa.dhs.gov	None
Preparation	Cyber Exercises	CISA	Free	Central@cisa.dhs.gov	None
Preparation	Information/Threat Indicator Sharing	CISA	Free	Central@cisa.dhs.gov	None
Preparation	Situational Awareness Reports and Intel Products	MS-ISAC Center for Internet Security	Free	https://cisecurity.org/ms-isac	Membership
Preparation	IP Address & Domain Monitoring	MS-ISAC Center for Internet Security	Free	https://cisecurity.org/ms-isac	Membership
Preparation	Cybersecurity Awareness Toolkit	MS-ISAC Center for Internet Security	Free	https://cisecurity.org/ms-isac	Membership

LOCALITY ENGAGEMENT GUIDE



Preparation	Malware IP Address and Domain List	MS-ISAC Center for Internet Security	Free	https://cisecurity.org/ms-isac	Membership
Preparation**	Penetration Tests	MS-ISAC Center for Internet Security	Email for pricing	https://cisecurity.org/ms-isac	Offered to SLTT
Preparation	Phishing Engagements	MS-ISAC Center for Internet Security	Email for pricing	https://cisecurity.org/ms-isac	Offered to SLTT
Preparation & Recovery**	CIS CyberMarket – collaborative purchasing program	MS-ISAC Center for Internet Security	Email for pricing	https://cisecurity.org/ms-isac	Offered to SLTT
Identification	Image/Artifact Analysis	VITA, VFC, VSP, CISA, MS-ISAC	Free	vfc@vfc.vsp.virginia.gov	None
Identification	Criminal Investigation	VSP & FBI	Free	Contact local FBI Field Office or vfc@vfc.vsp.virginia.gov	None
Identification	Case Support to Investigative Agencies	VFC & VSP	Free	vfc@vfc.vsp.virginia.gov	None
Identification	Assist with Attribution	FBI	Free	Contact local FBI Field Office or vfc@vfc.vsp.virginia.gov	None
Identification	SOC/Computer Emergency Response Team (CERT) Incident Response, computer forensics, malware analysis	MS-ISAC Center for Internet Security	Free	https://cisecurity.org/ms-isac	None for SLTT
Identification	Malicious Code Analysis Platform (MCAP)	MS-ISAC Center for Internet Security	Free	https://cisecurity.org/ms-isac	Membership
Identification	Albert: CIS Network Monitoring	MS-ISAC Center for Internet Security	Email for pricing	https://cisecurity.org/ms-isac	Offered to US SLTT
Identification	Malware Analysis	CISA	Free	Central@cisa.dhs.gov	None
Containment & Eradication	Consultation and advisory assistance	All Federal, State, and Local Partners	Free	vfc@vfc.vsp.virginia.gov	None
Containment & Eradication	Deployment of personnel	VANG and CISA	Free	vfc@vfc.vsp.virginia.gov , webEOC request; Central@cisa.dhs.gov	See agency information sheets for thresholds and requirements regarding this type of assistance
Recovery	Utilization of VITA procurement framework to obtain expedited equipment	VITA	Email for pricing	https://www.vita.virginia.gov	None