**Emergency Response Damage Assessment Procedure Template**

# PURPOSE

To establish and document the procedures for assessing damage to “YOUR AGENCY NAME” facilities as the result of an emergency situation.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners).

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The Emergency Response Damage Assessment Procedure at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the IT Incident Response requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Roles** | “YOUR AGENCY NAME” Facilities Manager | Information Security Officer | Building Landlord | Director | Security and/or Damage Team | IT Engineers |
| **Tasks** |   |   |  |  |  |  |
| Category 1 & 2 emergency | A | I | R | R | R |  |
| Category 3 & 4 emergency | R | A | R |  | R | R |

# STATEMENT OF PROCEDURE

Damage assessment, in response to any emergency situation, will ultimately be handled via the appropriate “YOUR AGENCY NAME” staff. However, this procedure identifies those personnel functions responsible for initiating and reporting status of the situation. The initial response procedure can best be categorized into two groups.

1. **EMERGENCY CATEGORY DEFINITIONS**
	1. Category 1: A minor incident involving one division or building that can usually be resolved by the Facilities or Building Manager and would NOT warrant the activation of the Emergency Response Plan. Examples Include:
		1. Broken water pipe
		2. Non-hazardous material spill
		3. Building loss of heat, air conditioning, or electricity for several hours
	2. Category 2: A division or building incident that is serious in nature but which can be resolved by the Physical Security Manager, the Information Security Officer and the Facilities Manager using existing agency resources or limited outside help. A Category 2 incident is usually a single event that has a limited duration and does not directly impact the entire agency. Examples Include:
		1. Violent assault on a single person
		2. Extended, widespread power outages
		3. Minor fire confined to a room and does not involve hazardous chemicals
		4. Potential employee exposure to biological-chemical agents
	3. Category 3: A major emergency or crisis situation potentially impacting numerous persons or a sizeable portion of the agency and/or community. Category 3 emergencies may be single or multi-event situations and often require considerable coordination both within and outside the agency. Category 3 emergencies could include imminent events in the agency or in the general community that can develop into a major crisis or full disaster. Examples Include:
		1. Violent assaults affecting many persons, hostage incidents, hate crimes
		2. Limited, small scale threats or incidents of acts of terrorism or the use of weapons of mass destruction (e.g. chemical/biological release in one room)
		3. Destructive ice/windstorms or thunderstorms; major fire or explosion; contagious disease outbreak; domestic water contamination; natural gas line breaks requiring large area evacuations
	4. Category 4: A catastrophic event involving the entire agency and surrounding community. Immediate resolution of the disaster is beyond the emergency response capabilities of the agency and local resources. Examples of Category 4 incidents could include:
		1. Major earthquake, hurricane, flood or devastating tornado, which would require State and Federal disaster assistance
		2. Threats or incidents of acts of terrorism or the use of weapons of mass destruction affecting entire portions of the agency or surrounding community.
2. **EMERGENCY PERSONNEL**
	1. Category 1 and Category 2 Emergency – The principal participants for these two groups will include the following:
		1. “YOUR AGENCY NAME” Facilities Manager
		2. Building Landlord
		3. Director and Division Managers of the affected areas

The “YOUR AGENCY NAME” Facilities Manager will take the lead, working with the landlord and identifying and working with the appropriate director and division managersandon site security. If the emergency is impacting the Data Center, the “YOUR AGENCY NAME” Facilities Manager will involve the Physical Security Manager along with the Technical Damage Assessment Team.

* 1. Category 3 and Category 4 Emergency– The principal participants for these two groups include the following:
		1. “YOUR AGENCY NAME” Information Security Officer
		2. “YOUR AGENCY NAME” Facilities Manager
		3. Building Landlords
		4. Computer Services Facility Engineers

The “YOUR AGENCY NAME” Information Security Officer will take the lead, working with the “YOUR AGENCY NAME” Facilities Manager, the building landlord and the computer services facility engineers.

1. **EMERGENCY PROCEDURES**
	1. Categories 1 and 2
		1. The “YOUR AGENCY NAME” Facilities Manager will ensure the safety of life and life support systems first.
		2. The “YOUR AGENCY NAME” Facilities Manager will notify the building landlord(s) of the situation and get them involved.
		3. The building landlords will be in charge of initial actions, including the notification of proper authorities.
		4. The “YOUR AGENCY NAME” Facilities Manager is responsible for coordination with the building landlords as to further actions to be taken.
		5. The “YOUR AGENCY NAME” Facilities Manager will get the affected director and division managers involved. They will conduct a damage assessment of the situation. If the Data Center and/or any of its support systems are affected, the Facility Security Manager and the Technical Damage Assessment Team will be involved.
		6. Once the damage assessment is completed, the “YOUR AGENCY NAME” Facilities Manager and affected director will report the status to the appropriate level of management.
	2. Categories 3 and 4
		1. The “YOUR AGENCY NAME” Information Security Officer will ensure the safety of life and life support systems first.
		2. The “YOUR AGENCY NAME” Information Security Officer will get the “YOUR AGENCY NAME” Facilities Manager involved and activate the “YOUR AGENCY NAME” Emergency Management Team.
		3. The “YOUR AGENCY NAME” Facilities Manager will contact the building landlord(s), and coordinate all activities with them.
		4. The building landlords will be responsible for notifying the appropriate authorities and coordinating any and all necessary activities. Once the authorities have determined that “YOUR AGENCY NAME” Damage Assessment Teams can enter the building, the building landlord(s) will notify the “YOUR AGENCY NAME” Facilities Manager.
		5. The “YOUR AGENCY NAME” Facilities Manager will then notify two teams:
			1. Non-Data Center Team made up of appropriate directors and/or division managers whose areas were impacted.
			2. Data Center Team made up of the Central Data Center Operations division managers and facility engineers. Each team will report to the facility and conduct a damage assessment of their respective areas.
		6. Once each team completes its damage assessment, they will report status to the “YOUR AGENCY NAME” Facilities Manager.
		7. The “YOUR AGENCY NAME” Facilities Manager will report status back to the “YOUR AGENCY NAME” Emergency Management Team.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Emergency Response Employee Communications

“YOUR AGENCY NAME” Emergency Response Securing the “YOUR AGENCY NAME” Facility Procedure

“YOUR AGENCY NAME” IT Contingency Planning Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY NAME””)

*Code of Virginia, §2.2-2009, et seq.*

(Additional duties of the CIO relating to security of government databases)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 01/13/2004 | Original under “YOUR AGENCY NAME” formatting and standardization. |
| 2 | 08/04/2004 | Administrative changes. |
| 3 | 11/19/2012 | Administrative changes. |
| 4 | 07/01/2014 | Formatting changes and role matrix added. |
| 5 | 11/09/2021 | Formatting changes |