# Cornell University
# PREVENTION AND MITIGATION PLAN

## Table of Contents

*Table of Contents*

# Section 1
# Prevention-Mitigation Introduction

As part of Cornell University's Emergency Management Plan, a prevention-mitigation program has been established to decrease the likelihood that an event or crisis will occur and to eliminate or reduce the loss of life and property damage related to an event or crisis. In order to drive prevention and mitigation activities, a Risk Assessment of the University's assets has been developed and maintained. Prevention programs and activities are distributed throughout campus health, safety and security departments.

# Section 2
# Risk Assessment

## 2.1 Risk Assessment Components

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence (occurrence), as determined by its likelihood and associated consequences. Major components of risk include:

- **Assets** that could be persons, structures, facilities, information, materials, and/or processes that have value.
- **Threats/hazards** that could include an occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerabilities** that could include physical features or operational attributes that render an asset open to exploitation or susceptible to a given hazard
- **Consequences/impacts** for the threats/hazards if they occur for particular assets.

## 2.2 University Risk Assessment Team

The University's Risk Assessment team is facilitated by Environmental Health and Safety and includes representatives from each of the Emergency Support Functions as outlined in the Emergency Operations Plan. The Risk Assessment Team is responsible for:

- Developing the list of University assets;
- Developing the characterization criteria;

- Conducting the assessment; and
- Maintaining the assessment.

## 2.3 Risk Assessment Methodology

The University's Risk Assessment Methodology includes a seven step process to identify and assess risks and to form priorities, develop courses of action, and inform decision-making. The methodology also includes a model to compute the data gathered during the risk assessment methodology into a quantitative risk score/ranking. The steps in the methodology includes:

1) Asset Identification
2) Threat/Hazard Characterization
3) Threat/Hazard Assessment
4) Vulnerability Assessment
5) Consequence Assessment
6) Risk Ranking
7) Countermeasures Assessment

For the threat/hazard, vulnerability, and consequence assessments the risk scoring/ranking scheme was based on a five point scale:

- Very low (1);
- Low (2);
- Medium (3);
- High (4); and
- Very high (5).

### 2.3.1 Asset Identification

University assets include persons, structures, facilities, information, materials, and/or processes that have value. For the University's Risk Assessment, assets were assessed from a categorical perspective campus-wide. Assets include:

| **Asset Category** | **Asset** |
|---|---|
| Persons | Employees (faculty & staff) |
| | Students |

| Asset Category | Asset |
|---|---|
| | Visitors |
| Facilities | Academic |
| | Athletic |
| | CUHA / NYS Veterinary Diagnostic Lab |
| | Data Center |
| | Dining / retail |
| | Emergency services |
| | Health centers |
| | Libraries |
| | Mass Assembly Area |
| | Military (ROTC) |
| | Natural areas |
| | Office |
| | Religious |
| | Research, general |
| | Research, specific |
| | Agricultural |
| | Animal |
| | Laboratories |
| | Biosafety – Select Agents / BSL3 / BSL1 or 2 |
| | Chemical |
| | Radiation – Irradiators / Radiation Use |
| | Residential |
| Infrastructure | Communications |
| | Data |
| | Protection systems |
| | Radio |
| | Telephony |
| | Grounds |
| | IT systems |

| Asset Category | Asset |
|---|---|
| | Business Data |
| | Computers |
| | IT Infrastructure (network, routers) |
| | Transportation |
| | Utility Distribution Systems |
| | Chilled water (main supply lines & balance distribution) |
| | Electric (main supply lines & balance distribution) |
| | Natural Gas Low pressure distribution |
| | Potable Water (Primary transmission and storage & Balance of distribution) |
| | Sewer collection (sanitary and storm) |
| | Steam (main supply lines & balance distribution) |
| | Utility Production/Sources |
| | Chilled water (LSC and CWP3 & TST) |
| | Maple Avenue Substation |
| | Potable water plant and other municipal sources |
| | Steam/Electric Facility |
| | Main production facility |
| | Main gas line |
| | Fuel oil storage |

### 2.3.2 Threat / Hazard Characterization

Threats / hazards are sources or causes of harm or disruption to the University's assets. Threats and hazards were developed based on the unique characteristics of the Ithaca campus. Categories included:

- Natural;
- Human-related;
- Terrorism; and
- Technological.

| Threat/Hazard Category | Threat/Hazard |
|---|---|
| **Natural** | Animal disease / infestation |
| | Dam break |
| | Drought |
| | Earthquake |
| | Flood |
| | Human infectious disease outbreak |
| | Inclement weather |
| | Land Movement |
| | Plant disease outbreak |
| | Severe storm |
| | Wild land fire |
| **Human Related** | Active shooter |
| | Activists/demonstration |
| | Aircraft crash |
| | Arson |
| | Assault |
| | Fraud |
| | Hazardous materials accident/spill |
| | Intentional Property Damage |
| | Internal sabotage to systems/services |
| | Labor action |
| | Riot |
| | Sabotage |
| | Suicide |
| | Theft |
| | Unintentional occurrence (food outbreak, accidental fire) |
| **Terrorism** | Chemical/biological/radioactive release |
| | Food/water/air contamination |
| | Improvised explosive device (IED) |
| | Radical Recruiting (CUPD TBD) |

| Threat/Hazard Category | Threat/Hazard |
|---|---|
| | Suicide bomber/multiple backpack bombs |
| **Technological** | Failure of the following: |
| | Chilled water |
| | Electrical |
| | Natural gas |
| | Outside service providers |
| | Sewer |
| | Steam |
| | Water |
| | Hazardous materials/energy release |
| | IT |
| | Computer virus |
| | Cyber Attack |
| | Denial of service attack |
| | Hardware failure |
| | IT cable break/damage |
| | Outside connectivity from disruption or failure |
| | Portable data loss/theft |
| | Security breach/hack |
| | Software bug |
| | Loss of structural integrity |
| | Structural fire |

## 2.3.3 Threat / Hazard Assessment

The threat/hazard assessment is the process of identifying or evaluating entities, actions, or occurrences, whether natural or human-caused, that have or indicate the potential to harm life, information, operations, and/or property.

The Threat / Hazard evaluation criteria used by the Risk Assessment Team includes:

Natural

| Factor | Code | Description |
|---|---|---|
| 1 | Very Low | Asset is located in an area that is not susceptible to specified natural hazard/event |
| 2 | Low | Natural hazard/event has occurred in asset area |
| 3 | Medium | Asset has experienced effects/loss from natural hazard/event |
| 4 | High | Asset has experienced effects/loss from natural hazard/event on multiple occasions |
| 5 | Very High | Asset regularly (at least every 5 years) experiences effects/loss from natural hazard/event |

Human-related

| Factor | Code | Description |
|---|---|---|
| 1 | Very Low | •No history of actual hazard occurring for the asset<br>•No credible evidence of capability or intent to threaten asset or similar asset<br>•Individuals would have no degree of interest in the asset |
| 2 | Low | •Low hazard for the asset<br>•Few known adversaries would pose a threat to the asset or similar asset<br>•Individuals would have some degree of interest in the asset |
| 3 | Medium | •Possible hazard for the asset<br>•Some known adversaries have desire to threaten asset or similar assets<br>•Individuals would have a moderate degree of interest in the asset |
| 4 | High | •Probable hazard exists for the asset<br>•Credible knowledge of adversary's capability and intent to threaten the asset or similar assets<br>•Individuals would have a high degree of interest in the asset |
| 5 | Very High | •History of actual hazard occurring for the asset<br>•Adversary demonstrates the capability and intent to threaten the asset or the asset is targeted frequently<br>•Individuals would have a very high degree of interest in the asset |

Terrorism

| Factor | Code | Description |
|---|---|---|
| 1 | Very Low | •No credible evidence of capability or intent; no history of actual or planned threats against the asset or similar assets<br>•Adversary would have no degree of interest in the asset |
| 2 | Low | •Low threat against the asset or similar assets and that few known adversaries would pose a threat to the assets<br>•Adversary would have some degree of interest in the asset |
| 3 | Medium | •Possible threat to asset based on adversary's desire to compromise similar assets<br>•Adversary would have a moderate degree of interest in the asset |
| 4 | High | •Credible threat exists against the asset based on knowledge of the adversary's capability and intent to attack the asset or similar assets<br>•Adversary would have a high degree of interest in the asset |
| 5 | Very High | •Credible threat exists against the asset and that the adversary demonstrates the capability and intent to launch an attack, and the asset is targeted frequently<br>•Adversary would have a very high degree of interest in the asset |

Technological

| Factor | Code | Description |
|---|---|---|
| 1 | Very Low | •Not susceptible to/affected by technological hazard<br>•Lack of infrastructure and/or new construction. Minimal stress factors Maintained regularly |
| 2 | Low | •Minimally susceptible to/affected by technological hazard<br>•Minimal infrastructure/engineering could fail. Relatively new construction<br>•Minimal stress factors. Maintained regularly |
| 3 | Medium | •Susceptible to/affected by technological hazard<br>•Some infrastructure/engineering could fail. Recent construction<br>• Moderate stress factors. Maintained as needed |
| 4 | High | •Has been affected by technological hazard<br>•Significant amount of infrastructure/engineering could fail. Old construction<br>•High stress factors. Maintained as needed |
| 5 | Very High | •Regularly affected by technological hazard<br>•Extremely high amount of infrastructure/engineering could fail. Very old construction<br>•Extreme stress factors. Not well maintained. |

## 2.3.4 Vulnerability Assessment

The vulnerability assessment identifies physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards.

Vulnerability includes two main components of accessibility and security posture. Accessibility of an asset factors how easily a natural, human-related, terrorism, or technological threat / hazard can expose an asset. Security posture relates to how effective the design of the asset is in protecting against a particular threat / hazard typically related to physical and information technology.

Accessibility

| Factor | Code | Description |
|---|---|---|
| 1 | Very Low | •N/A<br>•Protected from elements.<br>•No access/no public access/positive access controls implemented.<br>•Location not readily susceptible to threat/hazard. |
| 2 | Low | •Mostly protected from elements.<br>•Access limited to authorized individuals/access monitored and controlled.<br>•Location slightly susceptible to threat/hazard. |
| 3 | Medium | •Moderately protected from elements.<br>•Access monitored and controlled.<br>•Location moderately susceptible to threat/hazard. |
| 4 | High | •Slightly protected from elements.<br>•Access monitored.<br>•Location susceptible to threat/hazard. |
| 5 | Very High | •Not protected from elements.<br>•Public access allowed/no access controls.<br>•Location very susceptible to threat/hazard. |

Security Posture

| Factor | Code | Description |
|---|---|---|
| 1 | Very Low | •N/A<br>•Secure perimeter with monitoring. Access control at perimeter and asset. Stationary and roving security force. Monitoring of the asset.<br>•Proactive cyber security/IT department. Corporate/company IT security policy.<br>•All NIST SP 800-53 controls implemented. |
| 2 | Low | •Stationary and roving security force. Access control to the asset. Monitoring of the asset.<br>•Proactive cyber security/IT department. Corporate/company IT security policy.<br>•Most NIST SP 800-53 controls implemented. |
| 3 | Medium | •Roving security force. Access control to the asset.<br>•Reactive cyber security/IT department. Corporate/company IT security policy.<br>•Some NIST SP 800-53 controls implemented. |
| 4 | High | •Roving security force. Minimal access control to the asset.<br>•Some type of IT department. Basic software/system security controls. |
| 5 | Very High | •Little or no access control to the asset.<br>•Little or no software/system security controls. |

## 2.3.5 Consequence Assessment

Assessment of consequences includes the process of identifying or evaluating the potential or actual effects of an occurrence and the impacts from the perspectives of life safety, financial, and reputation.

## 2.3.6 Risk Ranking

Assessments for each asset are averaged within each assessment include:

- Threat/hazards;
- Vulnerabilities; and
- Consequences.

Then a total Risk Ranking is calculated by the equation listed below:

- Risk = (Threat/Hazard) x (Vulnerabilities) x (Consequences) / 3

Risk Ranking can be used throughout all the Emergency Management Phases including:

- Prevention-Mitigation: developing countermeasures and potential migration measures with quantifiable risk avoidance, control/mitigation, or transference.
- Preparedness: prioritizing assets and threat/hazards for conducting various levels of exercises.

- Response: assessing what gaps the Emergency Operation Plan and Emergency Support Functions might have in relationship to current capabilities and to plan for the need of new capabilities.
- Recovery: inform the continuity and recovery planning process of potential issues that may challenge those efforts.

### 2.3.7 Countermeasure Assessment

In evaluating the Risk Ranking, the Risk Assessment Team will identify or evaluate the potential or actual effects of actions, measures, or devices that reduce risk where deemed appropriate. Some potential actions that could be taken include:

- Risk acceptance
- Risk avoidance
- Risk control/mitigation
- Risk transference

When evaluating potential countermeasures, the University should consider each of these potential actions and analyze their potential cost / benefit in developing or not developing prevention or mitigation strategies.

## 2.4 Maintenance

At a minimum the Risk Assessment Team should review and maintain the University's Risk Assessment bi-annually. The Risk Assessment can also be reviewed and updated more frequently as the need arises for major changes in assets, threat/hazards, vulnerabilities, or consequences. Environmental Health and Safety is responsible for administering the University's Risk Assessment data and facilitating the Risk Assessment Team in its review and maintenance.

# Section 3
# Prevention

Prevention is the action taken to decrease the likelihood that an event or crisis. The hazards the University seeks to prevent are defined through the risk assessment process. Prevention programs and activities are administered by various campus organizations.

## 3.1 Prevention Programs

### 3.1.1 Environmental Health and Safety

Environmental Health and Safety maintains various prevention programs related to maintaining a safe living, learning and working environment. Programs include but are not limited to:

- Fire Safety
- Laboratory and Research Safety
- Occupational Safety
- Environmental Compliance

### 3.1.2 Cornell Police

Cornell Police maintains various prevention programs related to personal safety and security. Programs include but are not limited to:

- Crime Prevention
- Traffic Safety

### 3.1.3 Gannett Health Services

Gannett Health Services maintains various prevention programs related to personal physical and emotional wellness. Programs include but are not limited to:

- General Health and Wellness
- Mental Health
- Health Promotions

# Section 4
# Mitigation

Mitigation is the action taken to eliminate or reduce the loss of life and property damage related to an event or crisis, particularly those that cannot be prevented. Mitigation activities are incorporated into University risk management, safety and compliance programs. Activities are administered by various campus departments responsible for University systems, equipment, and facilities.

## 4.1 Mitigation Activities

Mitigation activities may be developed in light of actual or potential threats and hazards to University assets. Consideration for specific mitigation activities should be given to:

- After Action Reports from actual University incidents
- After Action reports from University exercises
- University Risk Assessments
- Recommendations from Risk Management and Insurance
- Benchmarking with peer institutions
- Input from the Cornell Emergency Support Function Team
- Guidance from governmental agencies