



LAMAR UNIVERSITY

MEMBER THE TEXAS STATE UNIVERSITY SYSTEM™

**COMPREHENSIVE
EMERGENCY MANAGEMENT PLAN (CEMP)**

VOLUME I:

PREVENTION - MITIGATION PLAN

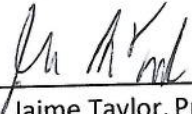
Publication Date: June 2019

Updated: July 2021

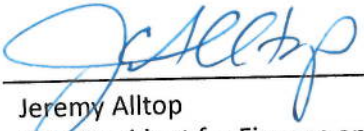


APPROVAL, SIGNATURES, AND IMPLEMENTATION

This Prevention – Mitigation Plan and its supporting contents are hereby approved, supersedes and rescinds all previous editions, and effective immediately upon the signing of all signature authorities noted below.

Approved: 
Dr. Jaime Taylor, President
Office of the President
Lamar University

Date: 7/24/2021

Approved: 
Jeremy Alltop
Vice President for Finance and Operations
Lamar University

Date: 01/29/2021



Table of Contents

| | |
|---|----|
| SECTION 1 – Prevention – Mitigation Introduction..... | 5 |
| SECTION 2 – Risk Assessment..... | 5 |
| 2.1. Risk Assessment Components..... | 5 |
| 2.2. University Risk Assessment Team | 5 |
| 2.3. Risk Assessment Methodology..... | 5 |
| 2.3.1 Asset Identification..... | 7 |
| 2.3.2 Threat / Hazard Characterization | 8 |
| 2.3.3 Threat / Hazard Assessment | 9 |
| 2.3.4 Vulnerability Assessment | 9 |
| 2.3.5 Failure Impact..... | 9 |
| 2.3.6 Risk Ranking..... | 10 |
| 2.3.7 Countermeasure Assessment..... | 10 |
| 2.4 Maintenance | 11 |
| SECTION 3 – Prevention | 11 |
| 3.1 Prevention Programs | 11 |
| 3.1.1 EHS & Risk Management | 11 |
| 3.1.2 Lamar University Police Department..... | 11 |
| 3.1.3 Student Health Center | 11 |
| SECTION 4 – Mitigation | 12 |
| 4.1. Mitigation Activities | 12 |



Section 1

Prevention – Mitigation Introduction

As part of Lamar University's Comprehensive Emergency Management Plan (CEMP), 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 Lamar University's assets has been developed and maintained.

Section 2

Risk Assessment

2.1 Risk Assessment Components

Risk is the potential for an unwanted outcome resulting from an incident, event, or 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

Lamar University's Risk Assessment team is facilitated by EHS & Risk Management and includes campus representatives. The Risk Assessment Team is responsible for:

- Developing the list of Lamar University assets
- Developing the characterization criteria
- Conducting the assessment
- Maintaining the assessment

2.3 Risk Assessment Methodology

Lamar University's Risk Assessment Methodology includes a five-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 of the methodology includes:

- Identify threats and hazards of concern
- Give the threats and hazards context



Prevention – Mitigation Plan

- Examine the core capabilities using the threats and hazards
- Set capability targets
- Apply the results

The following ten-point ranking systems will be used in the Risk Assessment Methodology:

| Likelihood of Occurrence | Value |
|---|-------|
| Extremely Likely (certainty; happens often) | 9-10 |
| Highly Likely (happens occasionally) | 7-8 |
| Probable (happened before; more than once) | 5-6 |
| Possible (happened many years ago) | 3-4 |
| Unlikely (no recent memory of this happening) | 1-2 |
| Does Not Happen | 0 |

| Vulnerability Table | Value |
|--|-------|
| Exceptionally grave vulnerability to threat or hazard, where future asset use is impossible | 10 |
| Grave vulnerability, where negative effect results in lack of asset use for extended period of time | 9 |
| Serious vulnerability, where negative effect results in lack of asset use for limited period of time | 8 |
| Serious vulnerability, where negative effect results in lack of asset use for minimal time | 7 |
| Moderate to serious vulnerability, where negative effect results in lack of asset use for slight delay | 6 |
| Moderate vulnerability, where negative effect results in no delay of asset use | 5 |
| Minimal vulnerability, where negative effect results in no delay of asset use | 4 |
| Minimal vulnerability or consequences, without negative long-term asset effect | 3 |
| Negligible vulnerability or consequences with minimal long-term asset effect | 2 |
| Negligible vulnerability or consequences without long-term asset effect | 1 |
| No consequences | 0 |

| Failure Impact Table | Value |
|---|-------|
| Exceptionally grave impact, where future asset use is impossible | 10 |
| Grave impact, where negative effect results in lack of asset use for extended period of time | 9 |
| Serious impact, where negative effect results in lack of asset use for limited period of time | 8 |
| Serious impact, where negative effect results in lack of asset use for minimal time | 7 |
| Moderate to serious impact, where negative effect results in lack of asset use for slight delay | 6 |
| Moderate impact, where negative effect results in no delay of asset use | 5 |
| Minimal impact, where negative effect results in no delay of asset use | 4 |
| Minimal impact or consequences, without negative long-term asset effect | 3 |
| Negligible consequences or impact with minimal long-term asset effect | 2 |
| Negligible consequences or impact without long-term asset effect | 1 |
| No consequences | 0 |



2.3.1 Asset Identification

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

| Asset Category | Asset |
|----------------|----------|
| Persons | Students |
| | Faculty |
| | Staff |

| Asset Category | Asset |
|----------------|----------------|
| Facilities | Administration |
| | Academic |
| | Athletic |
| | Dormitory |
| | Green Space |
| | Laboratories |
| | Parking Areas |
| | Residential |

| Asset Category | Asset |
|----------------|------------------------------|
| Infrastructure | Communications |
| | Data |
| | Protection Systems |
| | Radio |
| | Telephone |
| | Grounds |
| | Information Technology |
| | Business Data |
| | Computers |
| | Utility Distribution Systems |
| | Chilled Water |
| | Electric |
| | Natural Gas |
| | Potable Water |
| | Sewer |
| | Steam |
| | Fuel Storage |
| | |
| | |
| | |



2.3.2 Threat / Hazard Characterization

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

- Natural
- External
- Process

| Threat / Hazard Category | Threat / Hazard |
|--------------------------|--------------------------------|
| Natural | High Wind (Hurricane, Tornado) |
| | Winter Storm |
| | Drought |
| | Floods |

| Threat / Hazard Category | Threat / Hazard |
|---|---|
| External | Explosion – Nuclear Attack |
| | Explosion - Radiological |
| | Explosion – Incendiary Device |
| | Acts of Terror – Active Shooter/Armed Assault |
| | Chemical/Biological Event – Biological Outbreak |
| | Chemical/Biological Event – Food Contamination |
| | Chemical/Biological Event – Pandemic Influenza |
| | Chemical/Biological Event – Chemical Attack/Accident |
| | Chemical/Biological Event – Toxic Industrial Chemicals |
| | Infrastructure Attack/Failure/Damage – Power Outage/Blackout |
| | Infrastructure Attack/Failure/Damage – Communications System Disruption |
| | Infrastructure Attack/Failure/Damage – Water Supply Contamination/Sewer Failure |
| | Infrastructure Attack/Failure/Damage – Major Fire |
| | Infrastructure Attack/Failure/Damage – Heating/Air Conditioning Failure |
| | Infrastructure Attack/Failure/Damage – Ventilation System Failure |
| | Cyber Attack – Loss of Data or Network Service Disruption |
| | Cyber Attack – Control Systems Failure |
| | Economic/Labor/Insurrection – Civil Unrest |
| Economic/Labor/Insurrection – Workforce Strike | |
| Economic/Labor/Insurrection – Demonstration/Riot | |
| Economic/Labor/Insurrection – Economic Catastrophe (market crash) | |

| Threat / Hazard Category | Threat / Hazard |
|--------------------------|---|
| Process | Poor Process Design |
| | Failure to Make Timely Decisions |
| | Failure to Recognize Requirements/Obstacles |
| | Incompetence |



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:

| Likelihood of Occurrence | Value |
|---|-------|
| Extremely Likely (certainty; happens often) | 9-10 |
| Highly Likely (happens occasionally) | 7-8 |
| Probable (happened before; more than once) | 5-6 |
| Possible (happened many years ago) | 3-4 |
| Unlikely (no recent memory of this happening) | 1-2 |
| Does Not Happen | 0 |

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.

The vulnerability evaluation criteria used by the Risk Assessment Team includes:

| Vulnerability Table | Value |
|--|-------|
| Exceptionally grave vulnerability to threat or hazard, where future asset use is impossible | 10 |
| Grave vulnerability, where negative effect results in lack of asset use for extended period of time | 9 |
| Serious vulnerability, where negative effect results in lack of asset use for limited period of time | 8 |
| Serious vulnerability, where negative effect results in lack of asset use for minimal time | 7 |
| Moderate to serious vulnerability, where negative effect results in lack of asset use for slight delay | 6 |
| Moderate vulnerability, where negative effect results in no delay of asset use | 5 |
| Minimal vulnerability, where negative effect results in no delay of asset use | 4 |
| Minimal vulnerability or consequences, without negative long-term asset effect | 3 |
| Negligible vulnerability or consequences with minimal long-term asset effect | 2 |
| Negligible vulnerability or consequences without long-term asset effect | 1 |
| No consequences | 0 |

2.3.5 Failure Impact

Failure impact 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.

The failure impact criteria used by the Risk Assessment Team includes:



| Failure Impact Table | Value |
|---|-------|
| Exceptionally grave impact, where future asset use is impossible | 10 |
| Grave impact, where negative effect results in lack of asset use for extended period of time | 9 |
| Serious impact, where negative effect results in lack of asset use for limited period of time | 8 |
| Serious impact, where negative effect results in lack of asset use for minimal time | 7 |
| Moderate to serious impact, where negative effect results in lack of asset use for slight delay | 6 |
| Moderate impact, where negative effect results in no delay of asset use | 5 |
| Minimal impact, where negative effect results in no delay of asset use | 4 |
| Minimal impact or consequences, without negative long-term asset effect | 3 |
| Negligible consequences or impact with minimal long-term asset effect | 2 |
| Negligible consequences or impact without long-term asset effect | 1 |
| No consequences | 0 |

2.3.6 Risk Ranking

Assessment for each asset is the sum of the following categories:

- Threat / hazards
- Vulnerabilities
- Failure Impact

Risk Ranking is calculated by the below equation:

- Risk = (Threat / Hazard) + (Vulnerabilities) + (Failure Impact)

Risk Ranking can be used throughout the Comprehensive Emergency Management Plan:

- Prevention – Mitigation: developing countermeasures and potential migration measures with quantifiable risk avoidance, control/mitigation, or transference
- Preparedness: Prioritizing assets and threat / hazards for conducting levels of exercises
- Response: Assessing what gaps the Comprehensive Emergency Management Plan 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



2.4 Maintenance

At a minimum, the Risk Assessment Team should review and maintain Lamar 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 failure impacts. EHS & Risk Management is responsible for administering the 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 of an event or crisis. The hazards Lamar 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 EHS & Risk Management

EHS & Risk Management 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

3.1.2 Lamar University Police Department (LUPD)

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

- Crime Prevention
- Traffic Safety

3.1.3 Student Health Center

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

- General Health & 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 Lamar 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 Lamar University assets. Consideration for specific mitigation activities should be given to:

- After action reports for actual university incidents
- After action reports from university exercises
- University risk assessments
- Recommendations from EHS & Risk Management
- Benchmarking with peer institutions
- Input from Lamar University Executive Operations Team and Incident Management Team
- Guidance from governmental agencies