CyberSquad of Boone Inc.

Incident Management Plan

CYBER SQUAD

WE GOT YOUR BACK

Revision 1.0
June 2022

Revision History

Revision Date	Items Revised	Author
6/20/2022	Whole document	Gavin, Dylan, Ty, Derrick

Table of Contents

SECTION ONE -- PLAN BODY 5

1.1 Introduction 5
1.2 Incident Management Plan Overview 5
1.3 Scope 6
1.4 Exclusions 6
1.5 Planning Scenarios 6
1.5.1 Limited or No Access to the Building *6*
1.5.2 Loss of Data Communications, e.g., WAN, Routers *7*
1.5.3 Loss of Technology, e.g., Computer Room, Network Services *7*
1.5.4 Loss of People, e.g., Illness, Death *7*
1.6 Recovery Objectives 8
1.7 Assumptions 8

SECTION TWO -- INCIDENT RESPONSE AND MANAGEMENT 9

2.1 Logical Sequence of Events 9
2.2 Local Incident Management Teams 10
2.2.1 General Information *10*
2.2.2 Team Overview *11*
2.2.3 Local Incident Management Team *11*
2.2.4 Damage Assessment Team *11*
2.2.5 Regional Incident Management Team *11*
2.2.6 Threat Assessment Center *12*
2.3 Incident Management Team Activities 12
2.3.1 Local Incident Management Team Activities *12*
2.3.2 Regional Incident Manager Activities *12*
2.3.3 Regional Incident Management Executive Activities *12*

SECTION THREE -- NOTIFICATION, ESCALATION AND DECLARATION 13

3.1 Introduction 13
3.2 Notification Process Overview 13
3.2.1 Initial Notification *13*
3.3 Notification Process (Emergencies only) 14
3.3.1 Local IMT Notification and Notification of External Client, Vendor and Business Partner……….*14*
3.4 Incident Response Assembly Locations 15
3.5 Escalation Process (Emergencies only) 16
3.6 Plan Authorization and Declaration 17
3.7 Declaration Process (Emergencies Only) 17

SECTION FOUR -- INCIDENT RESPONSE CHECKLISTS 18

4.1 Key Personnel Contact List 18
4.2 Key Vendor Contact List 22
4.3 Initial Incident Response Checklist 23
4.4 Local Incident Management Team Task Checklist 24

4.4.1 Local Incident Management Team Meeting *25*
4.5 Local Incident Manager Task Checklist 25
4.5.1 Incident Response Recommended Actions *26*
4.5.2 Actions Following a Disaster Declaration *27*
4.6 Local Emergency Operations Center Command Staff Task Checklist 28
4.7 Local Emergency Operations Center Operations Staff Task Checklist 29
4.8 Pre-Incident Preparations 29

SECTION FIVE -- Red Team Policies **30**
5.1 Red Team Rules of Engagement 30

SECTION SIX -- Blue Team Policies **31**
6.1 Blue Team Rules of Engagement 31

SECTION SEVEN -- APPENDIXES **32**
7.1 Incident Management Forms 32

Section One -- Plan Body

1.1 Introduction

General Information

This manual was developed for CyberSquad of Boone, herein referred to as CSoB, and is classified as confidential property of that entity. Due to the sensitive nature of the information contained herein, this manual is available only to those persons who have been designated as members of one or more incident management teams or who otherwise play a direct role in the incident response and recovery processes.

Unless otherwise instructed, each plan recipient will receive and maintain two copies of the plan, stored as follows:

1. One copy at the plan recipient's office
2. One copy at the plan recipient's home

For additional copies, contact 336-555-0123.

The following teams will appear throughout this plan:

- Threat Assessment Center (TAC)
- Regional Incident Management Team (RIMT)
- Damage Assessment Team (DAT)
- Incident Management Team (IMT)

The incident management planning effort for CSoB recognizes and affirms the importance of people, processes and technology to the corporation.

It is the responsibility of each CSoB manager and employee to safeguard and keep confidential all corporate assets.

1.2 Incident Management Plan Overview

Overview and Objectives

This incident management plan establishes the recommended organization, actions and procedures needed to:

- recognize and respond to an incident;
- assess the situation quickly and effectively;
- notify the appropriate individuals and organizations about the incident;
- organize the company's response activities, including activating a command center;
- escalate the company's response efforts based on the severity of the incident; and
- support the business recovery efforts being made in the aftermath of the incident.

This plan is designed to minimize operational and financial impacts of such a disaster and will be activated when a local Incident Manager (or, in his/her absence, one of his/her alternates) determines that a disaster has occurred.

Specific details on incident response and subsequent business recovery actions and activities are included within the respective local recovery team plans.

1.3 Scope

This incident management plan includes initial actions and procedures to respond to events, such as the COVID-19 pandemic, that could impact critical business activities at the CSoB office in Boone, NC. This plan is designed to minimize the operational and financial impacts of such a disaster.

The CSoB Incident Management Plan is designed to provide an initial response to any unplanned business interruption, such as a loss of utility service, a major event like the COVID-19 pandemic or a catastrophic event, such as a major fire or flood. This document defines the requirements, strategies and proposed actions needed to respond to such an event.

1.4 Exclusions

This plan specifically excludes the following from its scope:

- facilities not located at the CSoB office in Boone, NC.

2.5 Planning Scenarios

This plan was developed to respond to an incident that could render the CSoB office in Boone, NC out of service or inaccessible. In addition, it is designed to respond to situations other than the above scenarios, e.g., the COVID-19 pandemic. The plan is designed to respond to scenarios such as the following:

- no access to buildings or floors at the specific location;
- loss of data communications and the network infrastructure;
- loss of technology; or
- loss of professional staff (e.g., via a flu outbreak).

1.5.1 Limited or No Access to the Building

Any incident that renders the CSoB office in Boone, NC either totally inaccessible/unusable or partially accessible to the tenants.

This scenario could produce one or more of the following impacts:

- loss of the business facility or the facility is rendered inaccessible;
- loss of access to selected workspace areas, such as building floors affected by a localized event, e.g., a fire;
- new equipment/facilities must be acquired;
- incident management and recovery actions must be implemented; or
- event causes business interruption or closing.

1.5.2 Loss of Data Communications, e.g., WAN, Routers

Any incident that disables or destroys the WAN router infrastructure and its communication capabilities located at CSoB office in Boone, NC, with a potentially disruptive effect on business operations.

This scenario could produce one or more of the following impacts:

- loss of access to the WAN;
- loss of access to the internet and intranet;
- incident is declared, and incident recovery actions are implemented;
- use of recovery strategies, commercial hot site, reciprocal agreements and manual operations as a temporary measure;
- business shutdown; or
- need for new facilities/equipment.

1.5.3 Loss of Technology, e.g., Computer Room, Network Services

Any incident that disables or destroys the entire computer room facility or its processing capacity located at CSoB office in Boone, NC, with a potentially disruptive effect on business operations.

This scenario could produce one or more of the following impacts:

- loss of use of the computer room facility;
- loss of voice/data communications services;
- incident is declared, and incident recovery actions are implemented;
- use of recovery strategies, commercial hot site, reciprocal agreements and manual operations as a temporary measure;
- business shutdown; or
- need for new facilities/equipment.

1.5.4 Loss of People, e.g., Illness, Death

Any incident that disables or renders the professional staff at CSoB office in Boone, NC unable to perform normal business functions, with a commensurate negative effect on business operations.

This scenario could produce one or more of the following impacts:

- no impact to building access or technology infrastructure;
- insufficient professional staff to perform minimal business operations;
- lack of suitably cross-trained staff;
- business shutdown; or
- need for temporary staff.

1.6 Recovery Objectives

This incident management plan has been developed to meet the following objectives:

- provide an organized and consolidated approach to managing initial response and recovery activities following an unplanned incident or business interruption, avoiding confusion and reducing exposure to error;
- provide prompt and appropriate response to unplanned incidents, thereby reducing the impacts resulting from short-term business interruptions;
- notify appropriate management, operational staff and their families, customers and public sector organizations of the incident; and
- recover essential business operations in a timely manner, increasing the ability of the company to recover from a damaging loss at Boone office.

1.7 Assumptions

This plan has been developed and is to be maintained on the basis of the following assumptions:

- A complete interruption of the CSoB office in Boone, NC office and associated facilities has occurred, and there is no access to the office, critical equipment or business data.
- A partial or total loss of professional staff at CSoB office in Boone, NC occurred due to employee illness resulting from a disaster, whether natural or man-made, including the COVID-19 pandemic or a similar outbreak, and only a limited number of healthy employees are available to continue normal business operations.
- Recovery from anything less than complete interruption will be achieved by using appropriate portions of this plan.
- Sufficient staff with adequate knowledge will be available to facilitate recovery.

Section Two -- Incident Response and Management

2.1 Logical Sequence of Events

The following high-level checklist describes the recommended emergency response.

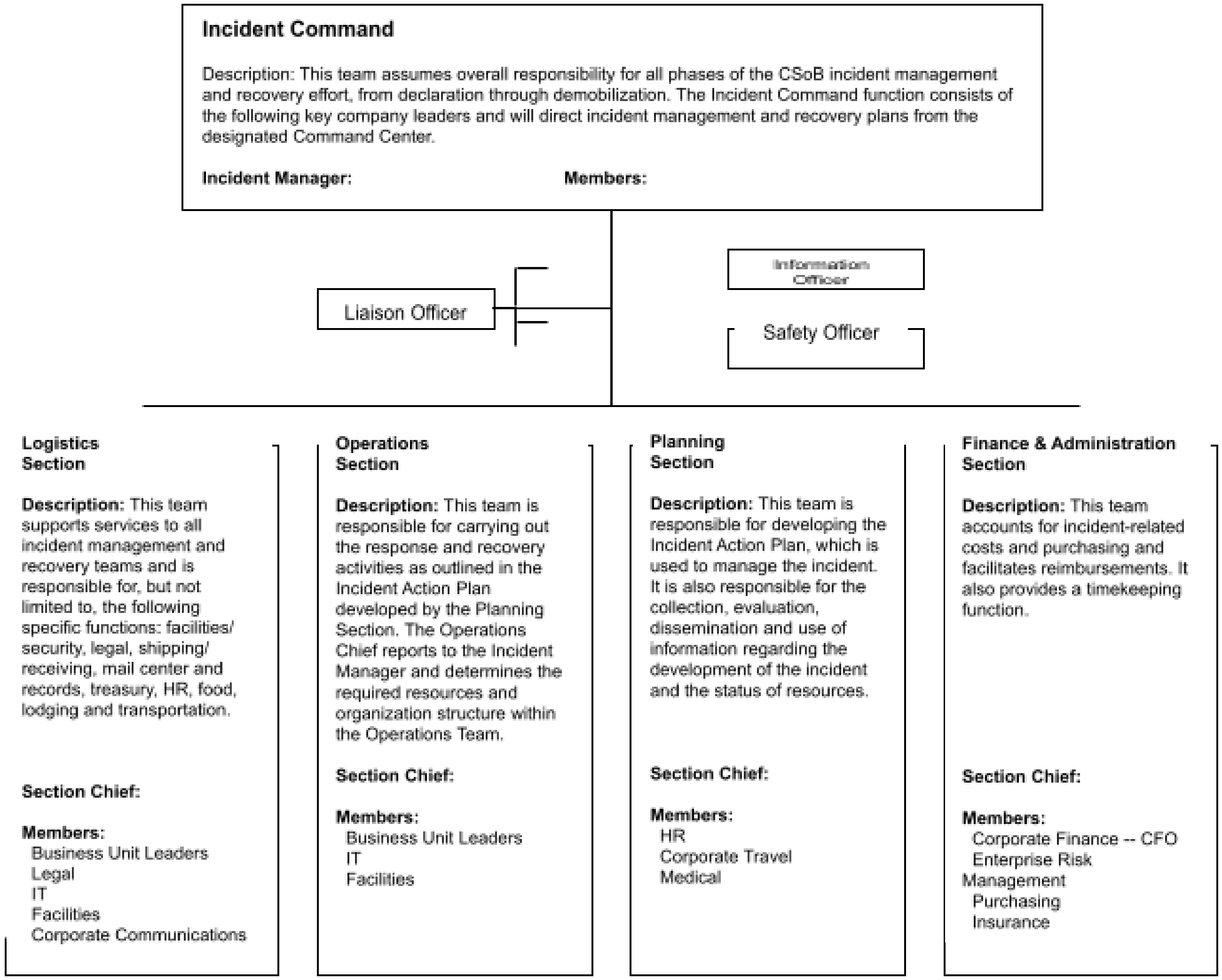
INITIAL INCIDENT RESPONSE CHECKLIST

Incident occurs.	□
First person to observe incident at Boone office follows local emergency procedures and notifies the local DAT and/or building security of incident.	□
The local DAT assembles, investigates the incident using a checklist and determines if the local IMT needs to be activated. If it is necessary, the DAT also notifies public authorities and/or dials 911.	□
If needed, the DAT will notify and activate the local IMT. The IMT designates a point of contact for the incident. The point of contact launches a notification process.	□
If life and safety are at immediate risk, the IMT Leader and his/her staff shall act first to ensure their own survival, as well as the survival of all staff, and then communicate when feasible.	□
As soon as possible, the IMT point of contact notifies the Regional Incident Manager (336-555-0123) and the TAC (336-555-0123) of the incident.	□
The TAC establishes local incident coordination with the IMT point of contact, assesses the incident and notifies senior management of the incident.	□
The Regional Incident Manager notifies the RIMT of the incident.	□
The TAC determines if the situation requires escalation, based on inputs from the DAT and IMT.	□
Assuming the situation warrants escalation, the IMT reviews the situation, briefs the TAC and Regional Incident Manager, and initiates the disaster declaration process.	□
If a disaster is not declared, the IMT point of contact advises the TAC and Regional Incident Manager.	□
If a disaster is declared, the local IMT: 1. notifies the TAC and Regional Incident Manager; 2. activates the Emergency Operations Center (EOC); 3. activates the Business Continuity - Incident Management plan; and 4. launches emergency response procedures.	□
The Regional Incident Manager consults with the TAC on the incident. Feedback from the TAC is relayed to local IMT point of contact.	□
All CSoB staff is notified of the incident and of operational status.	□
The incident management and business continuity plans continue until the incident has been resolved.	□

2.2 Local Incident Management Teams

2.2.1 General Information

A successful recovery from a disaster can only occur with total coordination of all incident management and recovery activities. In a crisis, each team has specific functions that contribute to the success of the recovery. The following diagram depicts the structure of a local IMT, particularly in the aftermath of an incident. It is based on the Incident Command System.



Incident Command

Description: This team assumes overall responsibility for all phases of the CSoB incident management and recovery effort, from declaration through demobilization. The Incident Command function consists of the following key company leaders and will direct incident management and recovery plans from the designated Command Center.

Incident Manager: **Members:**

Liaison Officer

Information Officer

Safety Officer

Logistics Section

Description: This team supports services to all incident management and recovery teams and is responsible for, but not limited to, the following specific functions: facilities/ security, legal, shipping/ receiving, mail center and records, treasury, HR, food, lodging and transportation.

Section Chief:

Members:
Business Unit Leaders
Legal
IT
Facilities
Corporate Communications

Operations Section

Description: This team is responsible for carrying out the response and recovery activities as outlined in the Incident Action Plan developed by the Planning Section. The Operations Chief reports to the Incident Manager and determines the required resources and organization structure within the Operations Team.

Section Chief:

Members:
Business Unit Leaders
IT
Facilities

Planning Section

Description: This team is responsible for developing the Incident Action Plan, which is used to manage the incident. It is also responsible for the collection, evaluation, dissemination and use of information regarding the development of the incident and the status of resources.

Section Chief:

Members:
HR
Corporate Travel
Medical

Finance & Administration Section

Description: This team accounts for incident-related costs and purchasing and facilitates reimbursements. It also provides a timekeeping function.

Section Chief:

Members:
Corporate Finance -- CFO
Enterprise Risk Management
Purchasing
Insurance

2.2.2 Team Overview

To implement the recovery strategies, the following teams are defined:

- Incident Management Team (IMT)
- Damage Assessment Team (DAT)
- Regional Incident Management Team (RIMT)
- Threat Assessment Center (TAC)

2.2.3 Local Incident Management Team

The local IMT assesses the physical and operational status of the Boone office immediately following an incident; determines the need for personnel evacuations; reviews the situation with building security and building management, as needed; reviews the situation with local public sector agencies (e.g., police, fire, EMT), as needed; provides input to the process for declaring a crisis or emergency, as needed; and organizes and deploys an EOC to manage all planning and operational aspects of the incident. The local IMT also makes an effort to reduce and control the impact of the incident to the Boone office.

Members:

Name	Office
Dylan Litaker	317

2.2.4 Damage Assessment Team

The DAT assesses the physical condition of the Boone office immediately following an incident; evaluates the damage and/or destruction to physical and technology assets to determine if an evacuation is indicated and what the prospects for recovery may be; reviews the situation with building security and building management, as well as local public sector agencies (e.g., police, fire, EMT), as needed; and provides input to and/or recommends a disaster declaration, as necessary.

Members:

Name	Office
Ty Brucker	317

2.2.5 Regional Incident Management Team

Composed of regional company executives and the Regional Incident Manager, the RIMT provides coordination and oversight during a regional incident that may affect an individual office or multiple offices in a geographic area.

Members:

Name	Office
Gavin Blankenship	317

2.2.6 Threat Assessment Center

The TAC provides a centralized and standardized means of validating and assessing threats and other incidents. Using information obtained from multiple sources, including local IMTs and Regional Incident Managers, the TAC provides single-source reporting to senior management and other stakeholders so that preemptive measures can be determined and implemented on a timely basis.

Members:

Name	Office
Derrick Hudson	317

2.3 Incident Management Team Activities

This plan provides detailed action steps for each member in the IMT structure.

2.3.1 Local Incident Management Team Activities

Detailed checklists that summarize recommended local IMT and leader activities can be found in Sections 4.4 and 4.5.

2.3.2 Regional Incident Manager Activities

Detailed checklists that summarize recommended Regional Incident Manager activities can be found in Section 4.6.

2.3.3 Regional Incident Management Executive Activities

Detailed checklists that summarize recommended RIMT executive activities can be found in Section 4.7.

Section Three -- Notification, Escalation and Declaration

3.1 Introduction

During any business interruption, **personnel safety** is the primary concern. Managers should periodically review emergency response and evacuation procedures with their staff to ensure familiarity with safety procedures.

Employees should notify their manager of any operational disruption or emergency situation. In the event of an emergency, CSoB managers Dylan Litaker, Ty Brucker, Derrick Hudson, and Gavin Blankenship are authorized to declare a disaster on behalf of the Boone office.

The notification plan is designed for use in mobilizing the IMT. If partial mobilization is needed, the appropriate portion of the plan can be executed accordingly. When primary IMT members cannot be reached for their part in the notification plan, their alternates will be contacted.

3.2 Notification Process Overview

3.2.1 Initial Notification

Telephone notification process

During normal business hours, contact personnel at the following numbers in the order listed:

- office telephone (if unavailable, leave a voicemail message);
- cellular;
- text (if available);
- home telephone; and
- any other number the person has listed in the employee's list.

During nonbusiness hours, contact personnel at the following numbers in the order listed until someone is reached:

- home phone;
- office (leave voicemail if no answer);
- cellphone/smartphone;
- text (if available); and
- any other number the person has listed in the disaster recovery documentation.

Automated notification process

When using an automated notification system during normal business hours, contact personnel at the following numbers in the order listed:

- office telephone (if unavailable, leave a voicemail message);
- cellphone/smartphone;

- text (if available);
- home telephone; and
- any other number the person has listed in the employee's list.

When using an automated emergency notification system during nonbusiness hours, contact personnel at the following numbers in the order listed until someone is reached:

- home phone;
- office (leave voicemail if no answer);
- cellphone/smartphone;
- text (if available); and
- any other number the person has listed in the disaster recovery documentation.

3.3 Notification Process (Emergencies only)

Communication during a crisis is critical. As such, follow local notification protocols in an emergency.

3.3.1 Local IMT Notification and Notification of External Client, Vendor and Business Partner

Should an incident occur, the following call tree will be utilized at Boone Office:

Temporary Staff				
Name	**Office Phone**	**Home Phone**	**Mobile**	**Location**
Rahman Tashakkori			336-555-1213	CSoB Boone office, room 317

3.4 Incident Response Assembly Locations

Primary Assembly Area

Name: Boone Office
Address: 110 Wallace circle
City/State/Zip: Boone, NC 28607
Phone/Fax: 828-792-3453
Email: litakerdc@appstate.edu

Secondary Assembly Area

Name: Wilkesboro Office
Address: 185 Ridgecrest St
City/State/Zip: Wilkesboro, NC 28697
Phone/Fax: 336-469-6872
Email: blankenshipgm@appstate.edu

Tertiary Assembly Area

Name: Fayetteville Office
Address: 6722B Irongate Dr
City/State/Zip: Fayetteville, NC 27332
Phone/Fax: 667-563-4578
Email: bruckert@appstate.edu

3.5 Escalation Process (Emergencies only)

The process for escalating an incident at CSoB is as follows:

1. Follow local established emergency escalation and life/safety protocols. If these are not available, the first CSoB employee to become aware of an incident should immediately report it to local management, who will escalate the information to the local IMT Leader Dylan Litaker or his/her designated alternate Gavin Blankenship.
2. Follow local established emergency escalation and life/safety protocols. If these are not available, the DAT should conduct an assessment of the situation. If the severity of the incident warrants, the IMT Leader or point of contact will inform the Regional Incident Manager, TAC, Business Continuity Management and CSoB management of the situation.
3. Follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of the local IMT assessment, and if the severity of the incident warrants, the Regional Incident Manager will coordinate with RIMT executives on the situation as soon as feasible by phone, email, audio conference or video conference (e.g., Zoom, Microsoft Teams).
4. Follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of the TAC assessment, and if the severity of the incident warrants, the TAC will notify designated senior management as deemed necessary to manage the situation; this can be done by phone, email, audio conference or video conference (e.g., Zoom, Microsoft Teams).
5. Continue to follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of local, regional and TAC discussions (via conference bridge and/or video conference), a decision will be made on declaring a disaster:
   a. IF a disaster IS NOT declared, the IMT Leader or Incident Manager will coordinate with other local management and Corporate Services staff to restore normal business operations accordingly.
   b. IF a disaster IS declared, the IMT Leader or Incident Manager, in coordination with the Business Continuity Team, will invoke the Business Continuity - Incident Management plan.
6. IF a declaration is made, the IMT point of contact will update the TAC, RIMT and CSoB management in Boone as soon as feasible.

3.6 Plan Authorization and Declaration

When the IMT is notified of the event, it will immediately contact the local business leadership on the incident, asking them to remain on standby. The IMT will report to the scene of the event, or where directed, and coordinate additional activities with local building management and the DAT. The call tree notification process begins after the authorization has been given to declare a disaster. Alternatively, if an automated notification system or service is available, launch that process as soon as possible.

3.7 Declaration Process (Emergencies Only)

The disaster declaration process at CSoB in Boone is as follows:

1. ONLY the management team in charge of CSoB or his/her appointed alternate has the authority to declare a disaster at CSoB.
2. A disaster declaration at CSoB MUST generally meet one or more of the following criteria:
   - The incident must qualify as a major, prolonged or indefinite disruption to business as usual.
   - The incident must be of sufficient magnitude (casualties/fatalities/property and/or facility damages/business disruptions, etc.) to warrant the enacting of emergency response and incident management measures to ensure continuity of operations at CSoB.
   - The incident has met and/or exceeded the threshold of disaster declaration criteria for appropriate major public sector entities on a local, regional, national or international level.
   - Not declaring the incident a "disaster" poses a direct threat to the viability of CSoB as a business.

Section Four -- Incident Response Checklists

4.1 Key Personnel Contact List

Incident Management Team							
Last Name	**First Name**	**Title**	**Department/Location**	**Work Phone**	**Home Phone**	**Alternate Phone**	**Mobile Phone**
Blankenship	Gavin	Manager	Regional Incident Management Team				336-469-6872
Litaker	Dylan	Manager	Local Incident Management Team				667-792-3453

Executive Management Team							
Last Name	**First Name**	**Title**	**Department/Location**	**Work Phone**	**Home Phone**	**Alternate Phone**	**Mobile Phone**
Brucker	Ty	Manager	Damage Assessment Team				
Hudson	Derrick	Manager	Threat Assessment Center				

4.2 Key Vendor Contact List

Vendor Name	Last Name	First Name	Title	Office Phone	Mobile Phone	Fax Number
App State	Tashakkori	Rahman	Chairman		336-555-1213	

4.3 Initial Incident Response Checklist

The subsequent task checklists should be followed in the event of an incident at the CSoB & Belk Hall office or surrounding area. Follow the recommended sequence of actions below during the initial minutes after the occurrence of an incident.

INITIAL INCIDENT RESPONSE CHECKLIST

Incident occurs.	□
First person to observe incident at a location follows local emergency procedures and notifies the local DAT and/or building security of incident.	□
The local DAT assembles, investigates the incident using a checklist and determines if the local IMT needs to be activated. If necessary, the DAT also notifies public authorities and/or dials 911.	□
If needed, the DAT will notify and activate the local IMT. The IMT designates a point of contact for the incident. The point of contact launches a notification process.	□
If life and safety are at immediate risk, the IMT Leader and his/her staff shall act first to ensure their own survival, as well as the survival of all staff, and then communicate when feasible.	□
As soon as possible, the IMT point of contact notifies the Regional Incident Manager (336-555-0123) and the TAC (336-555-0123) of the incident.	□
The TAC establishes local incident coordination with the IMT point of contact, assesses the incident and notifies senior management of the incident.	□
The Regional Incident Manager notifies the RIMT of the incident.	□
The TAC determines if the situation requires escalation, based on inputs from the DAT and IMT.	□
Assuming the situation warrants escalation, the IMT reviews the situation, briefs the TAC and Regional Incident Manager, and initiates the disaster declaration process.	□
If a disaster is not declared, the IMT point of contact advises the TAC and Regional Incident Manager.	□
If a disaster is declared, the local IMT: ● notifies the TAC and Regional Incident Manager; ● activates the EOC; ● activates the Business Continuity - Incident Management plan; and ● launches emergency response procedures.	□
The Regional Incident Manager consults with the TAC on the incident. Feedback from the TAC is relayed to local IMT point of contact.	□
All CSoB staff is notified of the incident and of operational status.	□
The incident management and business continuity plans continue until the incident has been resolved.	□

4.4 Local Incident Management Team Task Checklist

The following recommended sequence of actions should be facilitated after completion of the Initial Response Checklist in Section 4.3.

LOCAL INCIDENT MANAGEMENT TEAM TASK CHECKLIST

Gathers information about the incident from firsthand contact, available first responders, employees and others; relays to Incident Manager.	□
Accounts for all staff/guests on (and, if applicable, off) premises.	□
Administers first aid and/or ensures life/safety measures as appropriate.	□
Informs building security (336-555-0123) and the property management firm (336-555-0123), if they are not already aware of the incident.	□
Informs security (336-555-0123) of the situation as soon as possible.	□
Informs the Incident Manager (336-555-0123) as soon as possible.	□
Conducts an initial assessment of the incident's likely impact on local operations; coordinates with DAT.	□
Disseminates information to local employees on the incident.	□
Provides information about the incident to first responder organizations.	□
Establishes and maintains communications with the Regional Incident Manager, TAC and appropriate business unit(s).	□
Provides input as directed to the disaster declaration process.	□
If disaster is declared, supports the Incident Management plan response.	□
If a disaster is not declared, supports recovery from the incident and restores operations accordingly.	□
Supports launch of EOC according to Incident Management plan.	□
Provides ongoing review and analysis of incident(s) with dissemination of information to the staff, Regional Incident Manager and TAC as needed.	□
Coordinates with counterparts in other regions as part of ongoing incident analysis.	□
Coordinates with Operations Section leadership, as well as third-party organizations, to ensure required resources are in place and ready for delivery to affected venue.	□
Supports Public Information Officer, Safety Officer and Liaison Officer roles.	□
Supports management of the incident and restores operations accordingly.	□
Supports post-event demobilization plan as needed.	□
Assists the IMT and Incident Manager as directed.	□
Provides post-event report of activities.	□

4.4.1 Local Incident Management Team Meeting

Contact local IMT Leader to ensure that the IMT has set an initial meeting and venue. Ensure that the presence of IMT members is recorded using the EXHIBIT 4: IMT PERSONNEL ASSIGNMENT FORM found in the Recovery Forms section of this document.	☐
Ensure that any missing IMT members, their alternates and any additional personnel are notified of the meeting. See the KEY CONTACTS section of this guide for a complete list of IMT members, alternates and their contact information.	☐
Obtain a current situation report from the IMT and DAT. Address the following key issues: ● type of event (fire, tornado, terrorism, power outage, telecom outage, etc.); ● specific location of event, if known (building, floor, side of floor, etc.); ● magnitude of the event; ● time of event; ● suspected cause; ● emergency/evacuation procedures status; ● police and fire departments notified; ● injuries and fatalities; ● building access status (current access, near-term potential access); ● immediate impact to business operations; and ● potential for news media attention.	☐
Establish schedule of updates for the TAC to monitor ongoing emergency response procedures. Commence providing TAC updates.	☐
Ensure that a member of the local IMT documents, in chronological order, incident milestones and actions taken using the EXHIBIT 1: INCIDENT REPORT template found in the Recovery Forms section of this document. This form will be used as a tool to update the IMT, TAC and/or other senior management.	☐
If required, provide advice to local senior management about whether employees should be sent home. Local senior management will develop a statement, determine method of communicating updates and communicate to employees.	☐
Follow up to ensure that local management has decided whether or not to intercept 800# phone lines with a customized emergency voice recording.	☐
Follow up to ensure that local management has decided to launch/not launch the emergency notification service, in addition to/in lieu of 800# service arrangements.	☐

4.5 Local Incident Manager Task Checklist

The following recommended sequence of actions should be provided by the local IMT Leader and/or Incident Manager after completing the Initial Incident Response Checklist in Section 4.3.

LOCAL INCIDENT MANAGER TASK CHECKLIST

Assumes overall leadership of all incident management activities.	☐
Receives information about the incident from the IMT, first responders, employees and others; contacts the DAT.	☐
Delegates the accounting for of all staff/guests on (and, if applicable, off) premises.	☐
Ensures first aid is being provided; ensures life/safety measures are being delivered.	☐
Informs local Business Continuity Management Team (336-555-0123) of situation as soon as possible.	☐
In coordination with the DAT, assesses the incident's likely impact on local operations.	☐

If assessment of the incident suggests a serious event that could adversely impact operations, advises the TAC as soon as possible.	☐
Provides input as directed to the disaster declaration process.	☐
Based on input from Regional Incident Manager and the TAC, determines if/when to declare a disaster.	☐
If a disaster is declared, facilitates activation of Incident Management plan, informs others (the TAC, Regional Incident Manager) and launches call notification via emergency notification system or calling tree.	☐
If a disaster is not declared, manages recovery from the incident and restores operations accordingly.	☐
Leads the launch of EOC according to Incident Management plan; assumes role of Incident Manager.	☐
Leads the launch of Public Information Officer, Safety Officer and Liaison Officer.	☐
Ensures Public Information Officer establishes regularly updated communications with Incident Manager and other units, e.g., Regional Incident Manager, as needed.	☐
Manages the incident and restores operations accordingly.	☐

4.5.1 Incident Response Recommended Actions

The IMT Leader will develop recommendations for senior management on what overall response strategies should be implemented to facilitate the recovery of business operations in the most timely, efficient and cost-effective manner.	☐
Considers information gathered in earlier incident and damage assessments, including, but not limited to, the following: ● area(s) affected by the disaster; ● anticipated duration of incident; ● availability of required employees; ● any special timing issues, such as relationship to month-end, quarter-end, etc.; ● any special business issues (e.g., unusual business volume or backlog, unusual contractual obligations); ● regulatory obligations; ● salvageable equipment and supplies (as documented in the EXHIBIT 5: CRITICAL EQUIPMENT ASSESSMENT & EVALUATION FORM found in the Recovery Forms section of this document); ● availability of equipment and supplies at potential alternate or off-site locations; ● salvageable records required for recovery activities; and ● records that require intensive reconstruction activities.	☐
Develops critical business function recovery priority lists for the following periods: ● 8 hours ● 12 hours ● 24 hours ● 72 hours or longer	☐
Recommends to the Executive Management Team and TAC the location(s) where critical business functions and IT operations can be recovered based upon the following priority: ● return to building ● local sites ● other sites ● Vendor location in Boone	☐

4.5.2 Actions Following a Disaster Declaration

Based on responses from the TAC and input from local management and public sector organizations, the IMT Leader launches an incident management plan that facilitates a safe and rapid evacuation of staff and locates the safest venue to activate an EOC based on the following priority list: ● Boone, NC	□
If not already identified locally, the IMT Leader identifies and communicates the recommended assembly site(s) to local IMT members, local management, local public sector organizations and the Business Recovery Team.	□
Ensures that the local IMT convenes a meeting to review response and recovery options, EOC setup procedures and other related activities, as specified in the incident management plan.	□
Relays the current situation report from the TAC and/or the RIMT. General points to be covered include the following: ● type of event (fire, tornado, terrorism, power outage, telecom outage, etc.); ● specific location of event, if known (building, floor, side of floor, etc.); ● magnitude of the event; ● time of event; ● suspected cause; ● emergency/evacuation procedures status; ● police and fire departments notified; ● injuries and fatalities; ● building access (current access, near-term potential access); ● immediate impact to business operations; and ● potential for media (e.g., television, radio) attention.	□
Establishes a schedule for updates to the regional IMT(s).	□
Assigns an IMT member responsibility to document, in chronological order, incident milestones and actions taken using the EXHIBIT 1: INCIDENT REPORT template found in the Recovery Forms section of this document. This form will be used as a tool to update the TAC and other senior management.	□
Provides input to the TAC and/or Executive Management Team about whether employees should be sent home. The Executive Management Team will develop a statement, determine method of communication for further updates and communicate to employees, e.g., using emergency notification system or other approved service.	□
The IMT Leader will decide whether or not to intercept 800# phone lines with a customized emergency voice recording. Main message in the first 24 hours *"Welcome to* CSoB. *We're sorry, but our normal business operations have been interrupted due to a large meteor. Please be patient as we are making every effort to recover operations as soon as possible. We expect to resume normal operations on or about December 25th, 1961."* The following persons are authorized to implement this message: Name: Derrick Hudson — Name: Gavin Blankenship Work: 336-555-0123 — Work: 336-555-0123 Home: 336-555-0123 — Home: 336-555-0123 Mobile: 336-555-0123 — Mobile: 336-555-0123	□
Supports local Incident Managers as required.	□
Assists with acquisition of resources as needed.	□
Provides regular incident updates to the TAC.	□

Provides regular regional incident updates to the IMTs and points of contact.	□
Establishes communications process/timeline for the RIMT.	□
Coordinates phone calls and conference calls for the RIMT.	□

4.6 Local Emergency Operations Center Command Staff Task Checklist

Assuming an EOC is established by the local IMT Leader or Incident Manager, the following recommended sequences of actions should be facilitated by individuals assigned to the specific positions defined below.

INCIDENT MANAGEMENT TEAM PUBLIC INFORMATION OFFICER TASK CHECKLIST

When activated, establishes communications with organizations as indicated in incident management plan, e.g., the Incident Manager, local management, Regional Incident Manager and TAC.	□
Establishes regular time frames for reporting incident and recovery status to designated organizations.	□
Processes incoming messages from internal and external organizations, including police, fire, EMS and the media.	□
Coordinates activities with Liaison Officer.	□
Distributes approved messages to designated parties when directed.	□
Assists the IMT and Incident Manager as directed.	□
Provides post-event report of activities.	□

INCIDENT MANAGEMENT TEAM SAFETY OFFICER TASK CHECKLIST

When activated, monitors and manages physical safety conditions.	□
Develops measures to ensure safety of personnel.	□
Assists in the administering of first aid and/or ensures life/safety measures as needed.	□
Monitors EOC personnel for stress, etc.	□
Assists Incident Manager as directed.	□
Provides post-event report of activities.	□

INCIDENT MANAGEMENT TEAM LIAISON OFFICER TASK CHECKLIST

When activated, interfaces with any/all public sector entities as appropriate, e.g., police, fire, EMS, OEM and government agencies.	□
Disseminates information and messages to appropriate departments and individuals.	□
Coordinates activities with Public Information Officer.	□
Assists Incident Manager as directed.	□
Provides post-event report of activities.	□

4.7 Local Emergency Operations Center Operations Staff Task Checklist

Assuming an EOC is established by the local IMT Leader or Incident Manager, the following recommended sequences of actions should be facilitated by individuals assigned to the specific positions defined below.

PLANNING TEAM LEADER TASK CHECKLIST

When activated, prepares Incident Action Plan.	☐
Maintains situation and resource status.	☐
Coordinates business continuity management activities.	☐
Coordinates the preparation and dissemination of incident documentation.	☐
Provides location for subject matter and technical expertise.	☐
Prepares demobilization plan as needed.	☐
Assists Incident Manager as directed.	☐
Disseminates information and messages to appropriate departments and individuals.	☐
Provides post-event report of activities.	☐

LOGISTICS TEAM LEADER TASK CHECKLIST

When activated, organizes and coordinates the provision of services (HR, communications, medical, food, transportation and housing) and support (supplies, facilities and ground support) to the incident.	☐
Disseminates information and messages to appropriate departments and individuals.	☐
Assists Incident Manager as directed.	☐
Provides post-event report of activities.	☐

OPERATIONS TEAM LEADER TASK CHECKLIST

When activated, directs and coordinates all tactical operations associated with the incident.	☐
Disseminates information and messages to appropriate departments and individuals.	☐
Assists Incident Manager as directed.	☐
Provides post-event report of activities.	☐

FINANCE TEAM LEADER TASK CHECKLIST

When activated, facilitates various administration and financial activities.	☐
Monitors incident costs and maintains financial records.	☐
Addresses insurance and workers' compensation issues.	☐
Facilitates procurement activities, e.g., contracts.	☐
Monitors timekeeping and related activities.	☐
Disseminates information and messages to appropriate departments and individuals.	☐
Assists Incident Manager as directed.	☐
Provides post-event report of activities.	☐

4.8 Pre-Incident Preparations

Establish regional response plans and procedures for dealing with incidents.	□
Establish communications process for disseminating information about an incident to the RIMT.	□
Establish point of contact for compiling information on incidents and reporting to the TAC and senior management.	□
Train alternate(s) assigned as backup to Regional Incident Manager.	□

4.8.1 Actions Following an Incident and Prior to a Disaster Declaration Being Made

Gather input from the local IMT, DAT and local senior management.	□
Analyze the input, and complete an initial assessment of the situation. Attempt to determine the potential for an evacuation or other activity that would negatively impact operations at the site.	□
Forward the assessment results and any other intelligence to the TAC for analysis and action.	□
Coordinate incident analysis with regional peers.	□

4.8.2 Support for Local Incident Management Team Meeting

Contact the local IMT Leader via Public Information Officer to ensure that the IMT has set an initial meeting and venue.	□
Obtain a current situation report from the IMT and DAT. Key talking points include the following: ● type of event (fire, tornado, terrorism, power outage, telecom outage, etc.); ● specific location of event, if known (building, floor, side of floor, etc.); ● magnitude of the event; ● time of event; ● suspected cause; ● emergency/evacuation procedures status; ● police and fire departments notified; ● injuries and fatalities; ● building access status (current access, near-term potential access); ● immediate impact to business operations; and ● potential for news media attention.	□
Ensure creation of a schedule of updates for the TAC to monitor ongoing emergency response procedures. Commence providing the TAC updates.	□
Ensure a member of the local IMT documents, in chronological order, incident milestones and actions taken using the EXHIBIT 1: INCIDENT REPORT template found in the Recovery Forms section of this document. This form will be used as a tool to update the IMT, TAC and/or other senior management.	□
Ensure local management has decided whether or not to intercept 800# phone lines with a customized emergency voice recording.	□
Ensure local management has decided to launch/not launch the emergency notification service, in addition to/in lieu of 800# service arrangements.	□

4.8.3 Actions During and After the Disaster

Ensure Emergency Number 336-555-0123 is updated as follows: CSoB Regional Incident Manager: Office: 336-555-0123 Mobile: 336-555-0123 Home: 336-555-0123 CSoB VP: Office: 336-555-0123 Mobile: 336-555-0123 Home: 336-555-0123	□
Provide a brief situation report, including the following: ● nature of the incident (e.g., physical damage, life safety issues); ● potential impact to business units; ● actions taken by the local IMT and DAT; ● actions taken by local management; ● actions taken by employees; ● actions taken by others; and ● estimated time to return to normal operations.	□
Identify local EOC location and contact information.	□
Continue updates on agreed-upon schedule.	□
Follow up to ensure CSoB team leaders have notified their respective recovery team members. Document notifications in the EXHIBIT 3: PERSONNEL NOTIFICATION CONTROL LOG found in the Recovery Forms section of this document.	□
Notify any other CSoB contacts and third parties as deemed necessary. See the KEY CONTACTS section of this guide for contact information.	□
Follow up to ensure information regarding the status of the incident and the company's response to it is regularly communicated to the appropriate individuals and organizations.	□
Be available to answer questions and provide input to other organizations as they enter the incident response/recovery process.	□
Be available to answer questions and provide input to other organizations as they enter the post-incident recovery and evaluation process.	□

4.8.4 Post-Event Maintenance Activities

Assess regional incident management readiness.	□
Assess COVID-19 pandemic or similar event readiness in region.	□
Maintain Incident Management program through quarterly team training and updating of Incident Management plan documentation and checklists.	□

Section Five – Red Team Rules of Engagement

Executive Summary

The Rules of Engagement (ROE) document the approvals, authorizations, and critical implementation issues necessary to execute the engagement. Signing of the ROE constitutes acknowledgement and approval of the customer, system owner, and Red Team (made up of Derrick and Ty) of the Red Team's authorities in execution of the engagement.

Objectives:

- Exploit
- Compromise
- Circumvent

Explicit Restrictions:

- Any IP outside of range: 152.10.0.0/512
- Do not shut servers or infiltrated systems
- Do not change user passwords or system information

Authorized Target Space:

- IP Range: 152.10.0.0/512
- Building: Belk Hall, #317

Activities:

- Physical security breach
- Wireless access
- Email exploits and phishing
- Appropriate social engineering techniques for access

Red Team Tools:

- Metasploit
- Nmap
- Masscan
- Wireshark
- Nikto
- Social engineering
- tcpdump
- John the Ripper
- Nessus

Section Six – Blue Team Policy

Introduction

Blue teams (consisting of Gavin and Dylan) perform all of the SOC (security operations center) functions and are generally responsible for security information and event management (SIEM), incident tracking, threat intelligence, packet capture and analysis, and security automation. Additionally, blue teams identify critical assets and conduct intermittent risk assessments in the form of vulnerability scans and penetration testing to continually test their exposure.

The Three High-Level Phases:

- Current State
  - Assess current inventory & asset management
  - Asses current security posture & risk appetite
  - Asses current security Exposure
- Target State
  - Develop internal security offerings
  - Policies, controls, & procedures
  - Document desired state
- Implement & Integrate
  - Gap analysis
  - Implementation
  - Operations
  - Continuous program maturity

Blue Team Tools:

- Nmap
- Wireshark
- Syslog

Section Seven -- Appendixes

7.1 Incident Management Forms

Exhibit 1: Incident Report

Date	Nature of Incident	Time / Details	Action Taken	Directive

Exhibit 2: Incident Objectives & Strategy Form

Date/Time:				
Incident Name:				
Expected Duration:				
Completed By:				
Objectives/Strategies to be Completed in the First 3 Hours:				
Objectives/Strategies	IMT Leader	Assigned Date/Time	Status	Completed Date/Time
Objectives/Strategies to be Completed in the First 8 Hours:				
Objectives/Strategies	IMT Leader	Assigned Date/Time	Status	Completed Date/Time
Objectives/Strategies to be Completed in the First 15 Hours:				
Objectives/Strategies	IMT Leader	Assigned Date/Time	Status	Completed Date/Time
Objectives/Strategies to be Completed in the First 24 Hours & After:				
Objectives/Strategies	IMT Leader	Assigned Date/Time	Status	Completed Date/Time

Exhibit 3: Personnel Notification Control Log

Date/Time:					
Name	Status	Location Assignment	Phone Number	Work From	Work To

Exhibit 4: IMT Personnel Assignment Form

Date/Time:					
Incident Name:					
Recovery Team:					
#	**Name**	**Recovery Title / Role**	**Date/Time**	**Work From**	**Work To**
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					

Exhibit 5: Critical Equipment Assessment & Evaluation Form

Incident Name:				Date/Time:
Recovery Team:				Completed By:
Condition Key: *OK -- Undamaged* *DBU -- Damaged but usable* *DS -- Damaged; needs salvage before use* *D -- Destroyed*				
#	**Equipment (Itemize)**	**Condition**	**Time to Salvage**	**Comments**
1				
2				
3				
4				
5				
6				