INCIDENT CONTACT LIST

DATE UPDATED:____________

Corporate Security Officer:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:_________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: _____________________________________

____

Corporate Incident Handling, CIRT, or FIRST Team:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:_________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: _____________________________________

____

Corporate Legal Affairs Officer:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:_________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: _____________________________________

____

CIO or Information Systems Security Manager:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:_________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: _____________________________________

____

Corporate Public Affairs Officer:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:_________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: _____________________________________

____

Other (Specify):___________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:_________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: _____________________________________

____

INCIDENT CONTACT LIST

DATE UPDATED:____________

Local Contacts

Internet Service Provider Technical Contact:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:________________

E-mail: ______________________________________

Address: _____________________________________

____

Local FBI or Equivalent Agency:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:________________

E-mail: ______________________________________

Address: _____________________________________

____

Local Law Enforcement Computer Crime:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:________________

E-mail: ______________________________________

Address: _____________________________________

____

Local CIRT or FIRST Team:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:________________

E-mail: ______________________________________

Address: _____________________________________

____

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:________________

E-mail: ______________________________________

Address: _____________________________________

____

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:________________

E-mail: ______________________________________

Address: _____________________________________

____

INCIDENT CONTACT LIST

DATE UPDATED:____________

Other Contacts

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: ______________________________________

____

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: ______________________________________

____

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: ______________________________________

____

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: ______________________________________

____

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: ______________________________________

____

Other (Specify):____________________________

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:__________________

Fax:_________________ Alt. Fax:_________________

E-mail: ______________________________________

Address: ______________________________________

____

INCIDENT IDENTIFICATION

DATE UPDATED:____________

General Information

Incident Detector's Information:

Name:____

Title: ____

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:________________

Fax:_________________ Alt. Fax:________________

E-mail: _______________________________________

Address: ______________________________________

____

Detector's Signature:____________________________

Date and Time Detected: _________________________

Location Incident Detected From: _________________

____

Additional Information:__________________________

____

____

____

Date Signed: ___________________________________

Incident Summary

Type of Incident Detected:

- Denial of Service
- Malicious Code
- Unauthorized Use
- Unauthorized Access
- Espionage
- Other:_____________________________________
- Probe
- Hoax

Incident Location:

Site:____

Site Point of Contact:____________________________

Phone:______________ Alt. Phone: ______________

Mobile: ______________ Pager:________________

Fax:______________ Alt. Fax:________________

E-mail: _______________________________________

Address: ______________________________________

____

How was the Intellectual Property Detected:__________

____

____

____

____

____

____

____

Additional Information: ____

____

____

INCIDENT SURVEY

DATE UPDATED:____________

Location(s) of affected systems: ____

____

____

____

Date and time incident handlers arrived at site: ____________________________________

____

____

Describe affected information system(s) (one form per system is recommended):

Hardware Manufacturer:____

Serial Number: ____

Corporate Property Number (if applicable): ______________________________________

Is the affected system connected to a network? • **YES** • **NO**

System Name: ____

System Network Address:____

MAC Address: ____

Is the affected system connected to a modem? • **YES** • **NO**

Phone Number: ____

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etcetera):

____

____

____

____

____

____

____

____

____

.

INCIDENT CONTAINMENT

DATE UPDATED:____________

Isolate affected systems:

Command Decision Team approved removal from network? • YES • NO

If YES, date and time systems were removed: ____

If NO, state the reason: ____

____

____

Backup affected systems:

System backup successful for all systems? • YES • NO

Name of persons who did backup:____

____

____

____

____

Date and time backups started:____

Date and time backups complete: ____

Backup tapes sealed? • YES • NO Seal Date: _______________________

Backup tapes turned over to:____

Signature:____ Date: _______________________

Backup Storage Location: ____

INCIDENT ERADICATION

DATE UPDATED:____________

Name of persons performing forensics on systems: ____

____

____

____

____

Was the vulnerability identified? ● **YES** ● **NO**

Describe: ____

____

____

____

____

____

What was the validation procedure used to ensure problem was eradicated: ____________________________

____

____

____

____

____

____

____

INCIDENT COMMUNICATION LOG

DATE UPDATED:____________

Date:______________ **Time:**_________ • **am** • **pm** **Method (mail, phone, email, etc.):**________________

Initiator Name:__________________________________ Receiver Name:__________________________________

Initiator Title: __________________________________ Receiver Title: __________________________________

Initiator Organization: ___________________________ Receiver Organization:___________________________

Initiator Contact Info:____________________________ Receiver Contact Info: ___________________________

Details:____

____

____

____

Date:______________ **Time:**_________ • **am** • **pm** **Method (mail, phone, email, etc.):**________________

Initiator Name:__________________________________ Receiver Name:__________________________________

Initiator Title: __________________________________ Receiver Title: __________________________________

Initiator Organization: ___________________________ Receiver Organization:___________________________

Initiator Contact Info:____________________________ Receiver Contact Info: ___________________________

Details:____

____

____

____

Date:______________ **Time:**_________ • **am** • **pm** **Method (mail, phone, email, etc.):**________________

Initiator Name:__________________________________ Receiver Name:__________________________________

Initiator Title: __________________________________ Receiver Title: __________________________________

Initiator Organization: ___________________________ Receiver Organization:___________________________

Initiator Contact Info:____________________________ Receiver Contact Info: ___________________________

Details:____

____

____

____