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:	**Local FBI or Equivalent Agency:**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____
Local Law Enforcement Computer Crime:	**Local CIRT or FIRST Team:**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____
Other (Specify):_____	**Other (Specify):**_____
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	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:_____ Date and Time Detected: _____

Title: _____

Phone:_____ Alt. Phone: _____ Location Incident Detected From: _____

Mobile: _____ Pager:_____ _____

Fax:_____ Alt. Fax:_____ Additional Information:_____

E-mail: _____ _____

Address: _____ _____

_____ _____

Detector's Signature:_____ Date Signed: _____

Incident Summary

Type of Incident Detected:

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

Incident Location:

Site:_____ How was the Intellectual Property Detected:_____

Site Point of Contact:_____ _____

Phone:_____ Alt. Phone: _____ _____

Mobile: _____ Pager:_____ _____

Fax:_____ Alt. Fax:_____ _____

E-mail: _____ _____

Address: _____ _____

_____ _____

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:____

____

____

____