Incident Report

Incident identification information

Who detected the incident?

Name:	
Title:	
Phone:	
Alt. Phone:	
Email:	
Address:	
Date/time detected:	
Location of incident:	
System or application name:	

Incident summary

What type of incident was it? (circle applicable)

Denial of service	Unauthorized use	Espionage	Probe
Malicious code	Unauthorized access	Hoax	Loss
Unplanned downtime	Malware	RansomWare	Theft
Other:			

Describe the incident

Names of other involved

Incident notification

Who will be notified of the incident? (circle applicable)

CTO	CEO / President
Security Incident Response Team	Application owners
Administration team	Application users
Human resources	Hosting provider
Legal counsel	Public affairs

Specifically name individuals or groups that should be notified

Explain why the above should be notified

Actions

Phase I - Identification measures

Phase II - Containment measures

Evidence collected (system logs, etcetera)

Phase III - Eradication measures

Phase IV - Recovery measures

Evaluation

How well did the workforce members respond?

Were the documented procedures followed? Were they adequate?

What information was needed sooner?

Were any steps or actions taken that might have inhibited the recovery?

What could the workforce members do differently the next time an incident occurs?

What corrective actions can prevent similar incidents in the future?

What additional resources are needed to detect, analyze and mitigate future incidents?

Other conclusions or recommendations:

Follow-up

This incident report will be reviewed by: (organization to determine)

- Security officer
- Privacy officer
- CTO
- Other

Name of the Reviewer if Other was selected:

Recommended actions to carry out:

Who completed this incident report?

Initial report completed by:	
Follow-up completed by:	