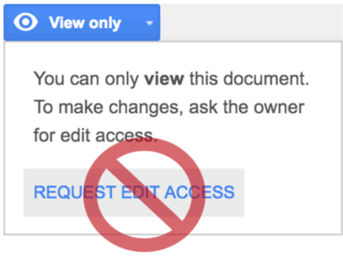


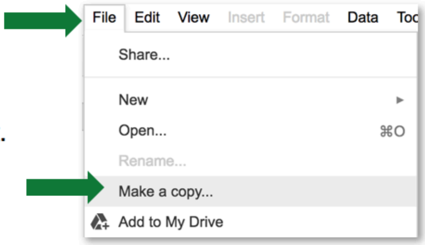
You can only **view** this document. To make changes, ask the owner for edit access.

How to use this template:

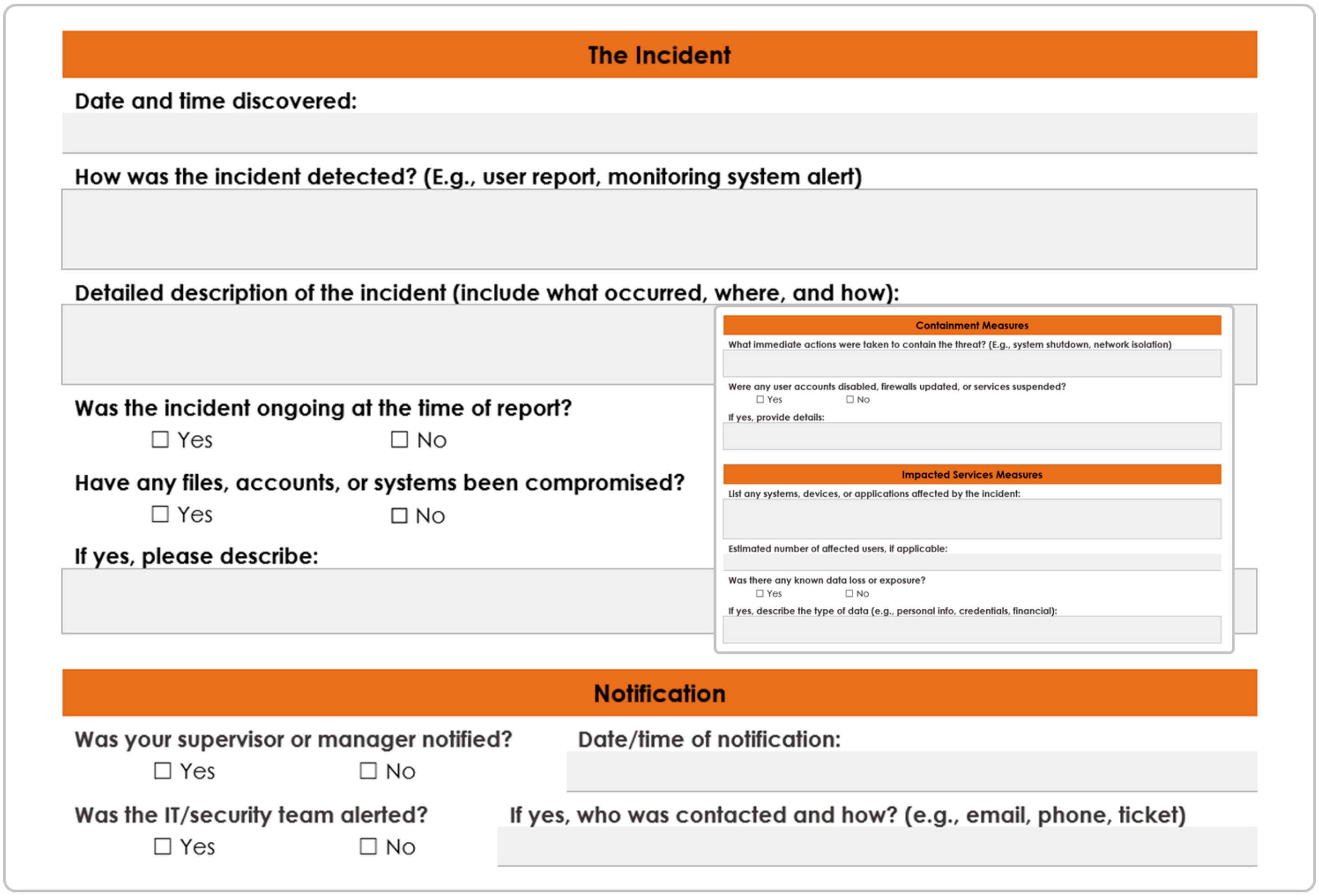
This is a view-only file and cannot be edited.

Create your own copy of this template to edit.

In the menu, click **File > Make a copy...**



Cybersecurity (IT) Incident Report Template



The Incident

Date and time discovered:

How was the incident detected? (E.g., user report, monitoring system alert)

Detailed description of the incident (include what occurred, where, and how):

Was the incident ongoing at the time of report?

☐ Yes ☐ No

Have any files, accounts, or systems been compromised?

☐ Yes ☐ No

If yes, please describe:

Containment Measures

What immediate actions were taken to contain the threat? (E.g., system shutdown, network isolation)

Were any user accounts disabled, firewalls updated, or services suspended?

☐ Yes ☐ No

If yes, provide details:

Impacted Services Measures

List any systems, devices, or applications affected by the incident:

Estimated number of affected users, if applicable:

Was there any known data loss or exposure?

☐ Yes ☐ No

If yes, describe the type of data (e.g., personal info, credentials, financial):

Notification

Was your supervisor or manager notified?

☐ Yes ☐ No

Date/time of notification:

Was the IT/security team alerted?

☐ Yes ☐ No

If yes, who was contacted and how? (e.g., email, phone, ticket)

Cybersecurity (IT) Incident Report Template

Confidential — *For Internal Use Only*

Use this form to document any IT-related security events, including unauthorized access attempts, data breaches, malware infections, phishing attacks, or any suspicious behavior potentially involving third parties. Timely reporting helps ensure that incidents are properly assessed, mitigated, and documented to reduce future risk. Please complete this report as soon as possible after the discovery of the incident.

Date of Report: ______________________

Contact Person

Full name

Job title / role

Department / team

Email address

Phone number

The Incident

Date and time discovered:

How was the incident detected? (E.g., user report, monitoring system alert)

Detailed description of the incident (include what occurred, where, and how):

Was the incident ongoing at the time of report?

□ Yes □ No

Have any files, accounts, or systems been compromised?

□ Yes □ No

If yes, please describe:

Notification

Was your supervisor or manager notified?

□ Yes □ No

Date/time of notification:

Was the IT/security team alerted?

□ Yes □ No

If yes, who was contacted and how? (e.g., email, phone, ticket)

Containment Measures

What immediate actions were taken to contain the threat? (E.g., system shutdown, network isolation)

Were any user accounts disabled, firewalls updated, or services suspended?

□ Yes □ No

If yes, provide details:

Impacted Services Measures

List any systems, devices, or applications affected by the incident:

Estimated number of affected users, if applicable:

Was there any known data loss or exposure?

□ Yes □ No

If yes, describe the type of data (e.g., personal info, credentials, financial):

Preliminary Analysis *(Optional)*

Suspected cause or entry point (e.g., phishing email, unpatched software):

Was the threat internal, external, or unknown?

□ Internal □ External □ Unknown

Submitted by:

Name **Signature** **Date submitted**

DISCLAIMER

Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk.