Cyber incident   
response plan template

*Fill in this template to create your cyber incident response plan or use it as a guide to write your own in a fresh document. Remember you can delete or edit anything that doesn’t feel relevant to your organisation.*

# 1. Incident response team

You and your employees need to know who to turn to when there is a cyber incident. Your incident response team will be responsible for:

* Making decisions
* Getting specialist help from outside your organisation
* Communicating about the incident
* Overseeing the response to fix the issue and get back to business
* Doing a post-incident review.

Your response team can include external IT support and other specialists.

### When creating your team, consider these questions:

* Who is allowed to make financial decisions?
* Who is responsible for technical decisions?
* Who will provide technical support? Is this person internal or external?
* Who is responsible for internal and external communication about the incident?
* Who in your organisation needs to be informed of an incident as soon as it happens?
* Who in your organisation needs to be updated as things change?

In your plan, include each person’s contact details, what they are responsible for and anything you need to know about how or when to contact them.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Job title | Working hours | Contact | Responsible for |
| *E.g. Marie Bani* | *Owner* | *9am–6pm* | *+679 111 1111* | *Financial decisions; reporting and external communications* |
| *E.g. Ailani Varu* | *Manager* | *9am–5pm* | *+679 222 2222* | *Organising tech support and making tech decisions; internal communications; post-incident review* |
| *E.g. IT Solutions Ltd* | *External IT provider* | *8am–6pm* | *+679 333 3333* | *Technical support, fixing the issue and technical recovery* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 2. Communications plan

### Internal communications

Outline a plan for communicating about incidents within your organisation. This could mean listing what kinds of incidents all staff need to be aware of, and any staff members who need to be told about all incidents.

You should also include your process and expected time frame for informing staff and consider how you will communicate with your team if devices aren’t working or your networks aren’t secure.

Larger organisations may like to develop some templates for what to say to staff in certain scenarios.

Regardless of your size, you should consider how you will communicate important information, such as:

* A summary of the incident and what it means for the business
* What is being done to resolve the issue
* What staff can do to help
* What staff should say if they are asked about the incident by customers or others outside the organisation
* Who staff should speak to if they have questions.

### External communications

Controlling the message with those outside of your organisation is vital for protecting your reputation and your ability to recover from an incident. You also have a duty to keep your customers and other stakeholders safe, by telling them if there has been an incident that might affect or harm them.

Your communications plan should include if, when and how you plan to tell your customers, the media, suppliers and other external stakeholders about an incident.

Think about what information different people need to know. For example, your customers will need to be informed if their sensitive information has been stolen, but they probably don’t need to know if the computers in your office aren’t working and it won’t impact them.

Consider how you will communicate relevant information such as:

* The systems/services affected or how the incident might affect them
* What is being done to resolve the issue
* Options for customers or other people affected
* Who to contact if they have questions.

You might have to deal with more complaints or questions from the public than usual, so consider how you will respond, what the best way for people to get in touch is, and if you’ll need extra resources, like staff or equipment.

You may like to create templates for what your staff should say in certain scenarios, or simply list guidelines.

# 3. Reporting processes

You might have legal obligations to report cyber incidents or information breaches. Reporting incidents to the police or your country’s national cyber security organisation can also help improve cyber security for the wider community.

List here who you need to report to, their contact details, what information needs to be included, and who is responsible for making the report.

You might include:

* The government or a specific department
* External stakeholders or customers
* Your insurance company, bank or internet service provider
* The police
* Your country’s national cyber security or ICT organization

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Report to (Organisation)** | **Contact details** | **When to report** | **Employee responsible** | **Notes** |
| *E.g. Industry regulator* | *https://industryregulator.org/report* | *Customers are affected (data breach)* | *Marie Bani* |  |
| *E.g. Financial Intelligence Unit* | *email@fiu.org* | *Money or financial details stolen* | *Marie Bani* |  |
| *E.g. Insurance company* | *+656 444 4444* | *All attacks* | *Marie Bani* |  |
| *E.g. The police* |  | *Threats, ransomware, theft* | *Marie Bani* |  |

# 4. Post-incident review and actions

Outline a process for what you will do after your organisation has recovered from the incident to learn from what happened and improve your cyber security and incident response.

This should include when and how you will conduct a post-incident review (PIR) or debrief and who should be involved. Specify what documents or types of actions should come out of the review, such as:

* A PIR report
* Updates to your cyber incident response plan based on what you’ve learnt
* Training for staff on cyber security awareness and any changes to your plan or procedures.

A PIR should answer these questions:

* How did the incident happen?
* Could the incident have been prevented? How?
* What did you do well in your response?
* What should you do differently to respond better to future incidents?

### Post-incident review template

*This template can be used to guide your review discussion or can be filled in after a debrief to create a PIR report. You can edit the template to better suit your organisation or a specific incident.*

|  |  |  |  |
| --- | --- | --- | --- |
| **INCIDENT SUMMARY** | | | |
| **Incident name/type** | |  | |
| **Date of incident** | |  | |
| **Personnel involved**  (Names and roles, including external service providers) | |  | |
| **Incident impact** | |  | |
| **Brief summary**  (What happened?) | |  | |
| **INCIDENT TIMELINE** | | | |
| **Date and time incident was discovered** | | *When did someone first notice there was an incident?* | |
| **Date and time of incident response** | | *When did you start actions to respond to the incident?* | |
| **Date and time of incident recovery** | | *When did you get your systems back to normal or resolve the issue?* | |
| **Who discovered the incident first and how?** | |  | |
| **Was the incident reported externally? If yes, when and to who?** | | *Did you report the incident to the police, your local CERT, a regulatory body or someone else?* | |
| **Who helped you to resolve the issue and when did they provide support?** | |  | |
| **What steps did you take to resolve the incident? When did you take these steps and what was the impact?** | | *List the time and impact of each step you took.* | |
| **How long did it take for all systems and networks to recover and business to go back to normal?** | |  | |
| **Actions to take:** | | *List what you can do to improve how quickly you respond to future incidents, such as training staff on how to spot incidents and who to call for help.* | |
| **PROTECTION** | | | |
| **What protections did you have in place to stop an incident like this?** | | *E.g. anti-virus software, secure customer networks.* | |
| **Did the protections work? Why/why not?**  **How can they be improved?** | |  | |
| **What processes or policies did you have in place to prevent an incident like this?** | | *List any organisational policies and procedures you had in place, such as staff cyber security training, a security strategy or mandatory multi-factor authentication.* | |
| **Did the processes work? Why/why not? How can they be improved?** | |  | |
| **Actions to take:** | | *List what you can do to improve protections against future incidents, like updating software or introducing better procedures.* | |

|  |  |
| --- | --- |
| **RESPONSE AND RECOVERY** | |
| **What was the cause of the incident?** |  |
| **How was the incident resolved?** |  |
| **What challenges did you face when responding to the incident?** |  |
| **Did you follow your organisation’s incident response plan or any other procedures?** | *Did they work? Why/why not?* |
| **Did you have the resources you needed to respond?**  (Including access to external support) |  |
| **How well did you share information and communicate within your organisation?** | *What worked well and what didn’t? Was information shared clearly and when it was needed? How could communications be improved?* |
| **Did you receive any media enquiries? If yes, what media and how did you respond?** |  |
| **Did you communicate with any customers or other external stakeholders about the incident?** | *Why/why not? When and how did you do this? What could be improved next time?* |
| **Actions to take:** | *List what you can do to improve how you respond to and recover from future incidents, such as updating your communications plan or more training for staff.* |

# + Other

You need to make your cyber incident response plan work for your organisation. You can include as much or as little information as you and your team need.

If you have other plans, policies or procedures in place, or government-wide guidance that you need to follow, you may want to include a list of these documents in your cyber incident response plan, including where they can be found when you need them.

You could also include:

* More detailed instructions for responding to specific incidents
* Plans for monitoring and detecting when incidents happen
* Templates for documenting incidents, your response and your recovery as they happen.