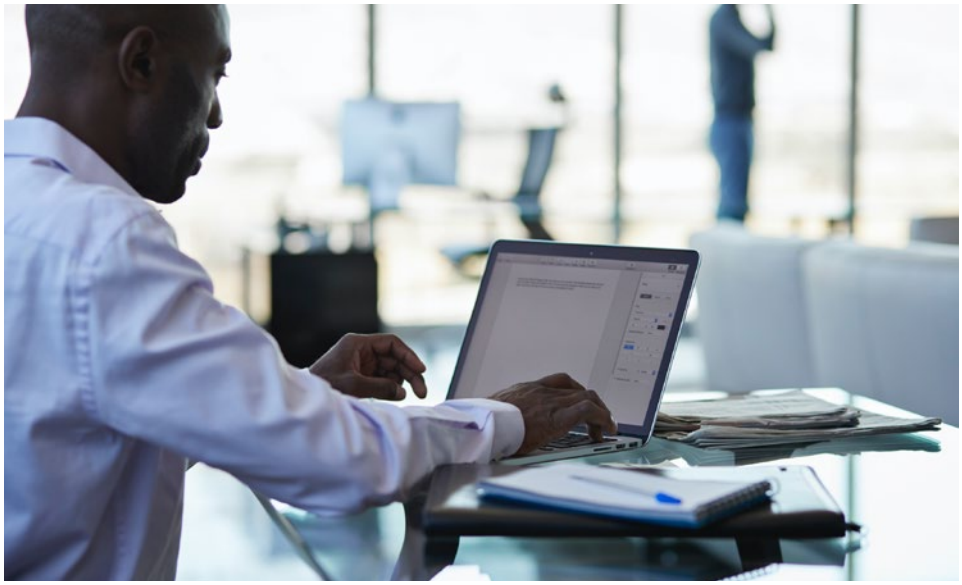
BlackBerry
Intelligent Security. Everywhere.

# IT and Cyber Incident Response Communication Templates



BlackBerry® Alert is a critical event management (CEM) solution designed to help organizations prepare for, respond to, and recover from disruptive events, enhancing operational resilience, reducing costs, and keeping people safer.

The intent of this communications guide response pack is to provide organizations with shared resources or dedicated functions, such as Incident Response (IR)/ Security Operations Center (SOC)/IT Security Coordinators, a rapid means of communicating key information to relevant stakeholders concerning cybersecurity and IT related events.

There are three basic scenario message templates for immediate deployment: **Cyber Incidents, Vulnerability Indicators of Compromise (IOC) Notices and IT Alerting**. Each scenario has a set of recommended guidelines to note prior to publication. Messages are generally divided into three phases of an activity/event: preparedness, response, and recovery.

BlackBerry Alert

THESE TEMPLATES ARE FOR EXAMPLE PURPOSES ONLY AND NEED TO BE TAILORED FOR YOUR BUSINESS AND COUNTRY

| S/N | NAME/TITLE | RECOMMENDED ISSUANCE |
|---|---|---|
| | **Cyber Incidents** | |
| 1 | BlackBerry Alert Mobile App Registration | Immediate |
| 2A | Information on Potential Cybersecurity Threat - XXX | When notified by regulatory authority or engaged managed services agent |
| 2B | Assessment on Potential Cybersecurity Threat - XXX | After assessment by SOC of IR team |
| 3 | <Snr Mgt> Notification and Assessment on Potential Cybersecurity Threat - XXX | After assessment by SOC or IR team |
| 4 | <All Staff> Notification on Potential Cybersecurity Threat - XXX | After assessment by SOC or IR team |
| 5 | On-Going Security Threat - XXX | When recommended by SOC or IR teams, or required by regulatory authority |
| 6 | Interim Update on Security Threat - XXX | When recommended by SOC or IR teams, or required by regulatory authority |
| 7 | Cybersecurity Threat XXX Resolution Status | When confirmed by SOC or IR teams, or recommended by regulatory authority |
| Should BCP be required for potential activation… | | |
| A1 | Preparation for Activation of BCP | In the event the cyber incident has the potential to involve or impact physical life and safety |

| | | | |
|---|---|---|---|
| A2 | Activation BCP - Work from Home |  | When an impact to life safety or threat to physical security on-site is confirmed, recommending closure of premises or at time of relevant declared health alert |
| A3 | Return to Work Premises |  | When return to work premises is deemed safe, ready for re-occupation, and business resumption |
| | **Vulnerability IOC Notices** | | |
| 1 | BlackBerry Alert Mobile App Registration |  | Immediate |
| 2A | Assessment on Vulnerability/IOC |  | When notified by NCTC, regulatory authority or engaged managed services agent |
| 2B | Action Required on Reported Vulnerability/IOC |  | After review and assessed by SOC or IR team or mandated by sector regulator |
| | **IT Alerting** | | |
| 1 | BlackBerry Alert Mobile App Registration |  | Immediate |
| 2 | Notification of IT Service Issue (Incident Number XXX) |  | Message is received after customer has completed online service request form |
| 3 | Completion of IT Issue (Incident Number XXX) |  | Upon completion by relevant IT Response team |

# Cyber Incidents

Scenario: Potential Cyber Incidents (for Incident Management)

Use Case:

This template assumes that the organization is required to link up with related agencies and/or partners to provide timely reporting during a cyber incident. This use case is relevant to organizations required to comply with prescribed cybersecurity frameworks, provide an essential service to regulated sectors or as required by upstream customers. Where orgnaizations do not have a SOC team or a threat has just occurred, refer to S/N 4 onwards.

Recommended Communications Guidelines:

- As soon as practicable, attempt to identify the type or nature of the security threat, the precautions needed to be taken, as well as the relevant containment measures to be taken.
- Determine the mandated reporting timeframes (for example, for regulatory compliance).
- Depending on the complexity of the security threat identified/ encountered, the proposed communication steps may need to be expanded or repeated until incident closure.
- If you have an existing response playbook/SOP, incorporate them in this template.

Note:

- The following are recommended messages to be sent as Alerts via BlackBerry Alert, based on the recommended frequency.
- Business leaders and dedicated coordinators are advised to revise/calibrate the message details in accordance to their endorsed response playbook and sector governance chapter (for example, the National Cyber Threat Response Center).
- An assumption is made in the provided template that cybersecurity-related intel is provided by a regulatory authority or outsourced managed services agent. As a cyber scenario, the response lead is undertaken by the SOC/IR/IT Security teams (where available).
- Depending on threat complexity and assessment, additional alerts should be inserted to execute overall joint incident management.
- Unless otherwise specified, all responses will be “(1) Acknowledged“, “(2) I need further clarification“, or “(3) I need to report a suspicious activity“.

# 1. BlackBerry Alert Mobile App Registration

**PHASE**
- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**
- Immediate

**SENT BY**
- BlackBerry Alert Administrator

**RECEIVED BY**
- All stakeholders who have yet to download the application.

**REMARKS**
N/A

**MESSAGE BODY**
The Blackberry Alert Mobile App can be downloaded onto your mobile device and used to receive notifications.

Follow the instructions attached to this email.

The Org Code is: (ORG CODE)

You will find the BlackBerry Alert Mobile app for iPhone:

https://apps.apple.com/us/app/blackberry-alert/id1551697059

You will find the BlackBerry Alert Mobile app for Android:

https://play.google.com/store/apps/details?id=com.blackberry.alert.prod

**MORE INFO LINKS / ATTACHMENTS**
N/A

## 2A. Information on Potential Cybersecurity Threat - XXX

**PHASE**
- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**
- When notified by the regulatory authority or engaged managed services agent

**SENT BY**
- Resilience office

**RECEIVED BY**
- SOC/Cyber/IT team

**REMARKS**
An assumption is made that the contact point with the local regulatory authority or managed services agent is the resilience office. After the assessment is complete, the resilience office will need to separately update the regulatory authority, or per in-house response framework.

**MESSAGE BODY**
Dear SOC/IR/Cyber Response Team,

We have received information from our Sector Regulator/Managed Services vendor that a potential cybersecurity threat “XXX“ has been detected on the horizon and has so far targeted businesses in our operating sector.

Known Behavior:

The threat has the following known characteristics...

Known Modus Operandii:

The threat has been known to infiltrate targeted systems via the following means...

Action Required:

Please review the attached threat intel and evaluate. Provide the threat assessment and recommendation to the Resilience Office by end of day. Should general recipients need to be notified, initiate BlackBerry Alert.

**MORE INFO LINKS / ATTACHMENTS**
<Include links to source of alert, relevant scenario playbook, security incident reporting form, etc.>

## 2B. Assessment on Potential Cybersecurity Threat - XXX

**PHASE**

- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**

- After the assessment by SOC or Incident Response team.
- If the threat has impacted potential safety and security, initiate message A1 concurrently.

**SENT BY**

- SOC/Cyber/IT team

**RECEIVED BY**

- Resilience office

**REMARKS**

The SOC will only take over incident management upon confirmation of threat occurrence.

**MESSAGE BODY**

Dear <Resilience Office>,

We have reviewed the threat intel and attached our recommendation. We will coordinate the relevant actions as follows:

a) Intensify scanning and monitoring efforts to received threat signature

b) Notify the Incident Commander/Duty Manager for resource coordination actions unique to this threat

<Indicate all generic steps here>

We will also liaise directly with the Regulator in event of a confirmed threat occurrence.

**MORE INFO LINKS / ATTACHMENTS**

<Attach completed assessment report>

## 3. <Snr Mgt> Notification and Assessment on Potential Cybersecurity Threat - XXX

**PHASE**

- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**

- After the assessment by the SOC or Incident Response (IR) team.
- If the threat has impacted potential safety and security, initiate message A1 concurrently.

**SENT BY**

- SOC/Cyber/IT team

**RECEIVED BY**

- Senior management and key vendors' IT lead using impacted application

**REMARKS**

Respective functional senior management will internally review their security ops processes and seek clarification from the SOC where required.

**MESSAGE BODY**

Dear <Senior Management/Upstream Client>,

We have received information that a potential cybersecurity threat "XXX" has been detected on the horizon and has so far targeted businesses in our operating sector.

Known Behavior:

The threat has the following known characteristics...

Known Modus Operandii:

The threat has been known to infiltrate targeted systems via the following means...

a) Should SOC notify you of a confirmed threat, do not turn on your machine until further advised via BlackBerry Alert.

b) Be prepared to disconnect your machine from the network.

c) Should you notice anything suspicious, immediately notify your supervisor and the security operations center.

d) Do not post the incident on your personal social media account.

For further clarification, contact SOC at <indicate contact number here>

**MORE INFO LINKS / ATTACHMENTS**

<Include links to source of alert, relevant scenario playbook, etc.>

## 4. <All Staff> Notification on Potential Cybersecurity Threat - XXX

**PHASE**
- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**
- After the assessment by the SOC or Incident Response team

**SENT BY**
- SOC/Cyber/IT team

**RECEIVED BY**
- Staff and vendors using impacted application

**REMARKS**
All staff will receive similar notification and will seek clarification with SOC or Resilience Office if needed.

**MESSAGE BODY**
Dear Recipient,

We have received information that a potential cybersecurity threat "XXX" has recently been targeting businesses in our operating sector.

Our SOC teams are monitoring the potential threat and we seek your cooperation in observing the following:

Recommended Response:

a) Should SOC notify you of a confirmed threat, do not turn on your machine until further advised via BlackBerry Alert.

b) Be prepared to disconnect you machine from the network.

c) Should you notice anything suspicious, immediately notify your supervisor and the security operations center.

d) Do not post the incident on your personal social media account.

For further clarification, contact SOC at <indicate contact number here>

**MORE INFO LINKS / ATTACHMENTS**
<Include links to source of alert, relevant scenario playbook, etc.>

## 5. Ongoing Security Threat - XXX

**PHASE**
- Response

**RECOMMENDED ISSUANCE AND FREQUENCY**
- When recommended by the SOC or IR Teams, or required by the regulatory authority.

**SENT BY**
- SOC/Cyber/IT team

**RECEIVED BY**
- Senior management, staff and vendors of the impacted application

**REMARKS**
N/A

**MESSAGE BODY**
Dear Recipient,

This is to inform you that the earlier reported cybersecurity threat "XXX" has been detected in our company's operating environment. Our SOC and IT Security teams are working to resolve the issue. As a precautionary measure, access to the following internal processes shall be offline for the next XX hours.

Staff requiring access to these processes shall use the following LINK as an interim measure. This is necessary as we work to contain the threat and ensure communications with our customers and partners remain undisrupted.

As a recap, please note the following:

a) Should SOC notify you of a confirmed threat, do not turn on your machine until further advised via BlackBerry Alert.

b) Should you notice anything suspicious, immediately notify your supervisor and the security operations center.

b) Do not post the incident on your personal social media account.

For further clarification, contact SOC at <indicate contact number here>

**MORE INFO LINKS / ATTACHMENTS**
<Include links to previous comms alert, relevant scenario playbook, security incident reporting form, etc.>

## 6. Interim Update on Security Threat - XXX

**PHASE**
- Response

**RECOMMENDED ISSUANCE AND FREQUENCY**
- When recommended by SOC or IR Teams, or required by regulatory authority.

**SENT BY**
- SOC/Cyber/IT team

**RECEIVED BY**
- Senior management, staff and vendors of the impacted application.

**REMARKS**
N/A

**MESSAGE BODY**
Dear recipient,

Following our earlier reported cybersecurity threat "XXX" detected in our company's operating environment, our SOC and IT Security teams are still working to resolve the issue. As a precautionary measure, access to the following internal processes shall be offline until further notice.

Staff requiring access to these processes shall use the following LINK as an interim measure. This is necessary as we work to contain the threat and ensure communications with our customers and partners remain undisrupted.

As a recap, please note the following:

a) Should SOC notify you of a confirmed threat, do not turn on your machine until further advised via BlackBerry Alert.

b) Should you notice anything suspicious, immediately notify your supervisor and the security operations center.

c) Do not post the incident on your personal social media account.

For further clarification, contact SOC at <indicate contact number here>

**MORE INFO LINKS / ATTACHMENTS**
<Include links to previous comms alert, relevant scenario playbook, security incident reporting form, etc.>

## 7. Cybersecurity Threat XXX Resolution Status

**PHASE**
- Recovery

**RECOMMENDED ISSUANCE AND FREQUENCY**
- When confirmed by the SOC or IR Teams, or recommended by the regulating authority

**SENT BY**
- SOC/Cyber/IT team

**RECEIVED BY**
- Senior management, staff and vendors of the impacted application

**REMARKS**
N/A

**MESSAGE BODY**
Dear Recipient,

This is to inform you that the earlier reported cybersecurity threat "XXX" detected within our company's operating environment has been contained. Our SOC and IT Security teams are following up on post-event investigations. Access to the following internal processes are now permissible.

While we investigate the incident, staff and partners are reminded to remain vigilant and keep your passwords secure and regularly updated.

Going forward, should you encounter any suspicious behavior in your work processing, notify your supervisor and SOC teams immediately.

**MORE INFO LINKS / ATTACHMENTS**
<Include links to previous comms alert, relevant scenario playbook, security incident reporting form, etc.>

**Should BCP be required for Potential Activation**

## A1. Preparation for Activation of BCP

**PHASE**
- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**
- In the event the cyber incident has the potential to involve or impact physical life and safety

**SENT BY**
- Resilience office

**RECEIVED BY**
- All staff and vendors

**REMARKS**
An assumption is made that the resilience office leads in overall business continuity efforts

**MESSAGE BODY**
As part of our organization's business continuity measure, we will be preparing to transit into either split operations, or remote working. The options will be based on our respective job functions.

As part of preparatory measures, all staff (and supporting vendors) are requested to observe the following:

a) Ensure you have a stable home internet/ Wi-Fi connection.

b) Ensure you have valid teleconferencing software installed.

c) Review, reschedule or postpone non-business critical meetings or discussions in the event of BCP activation. If required, opt in for telephone or video conferencing.

d) Ensure you can access our applications and files remotely.

e) Provide an available cellphone number to your Managers in event of BCP activation.

f) Ensure your device has been updated with the latest security patches.

As a gentle reminder, staff and vendors should be bringing their office IT devices/ laptops home at the end of each business day. Please adhere to internal security policy for your respective location for remote working.

**MORE INFO LINKS / ATTACHMENTS**
<Insert any IT requirement checklist or intranet link for remote working facilitation>

## A2. Activation of BCP – Work from Home

**PHASE**
- Response

**RECOMMENDED ISSUANCE AND FREQUENCY**
- When an impact to life safety or threat to physical security on-site is confirmed, recommending closure of premises, or at the time of a relevant declared health alert

**SENT BY**
- Workplace Safety & Healthy (WSH) Office

**RECEIVED BY**
- All staff and vendors

**REMARKS**
An assumption is made that the WSH Office leads ground operational efforts

**MESSAGE BODY**
To safeguard staff and partners' well-being, the organization will be activating its business continuity plan (work from home) procedure.

With effect from <indicate date>, all staff and supporting vendors will commence remote working. Ensure your contact details have been updated.

Staff and vendors are to conduct any required meetings and discussions via tele/video conferencing.

Please adhere to internal security policy for your respective location for remote working.

Check with your Managers or the IT team for further clarification or support.

Stay safe and vigilant.

**MORE INFO LINKS / ATTACHMENTS**
<Insert link to internal BCP>

## A3. Return to Work Premises

**PHASE**
- Recovery

**RECOMMENDED ISSUANCE AND FREQUENCY**
- When return to work premises is deemed safe, ready for re-occupation and business resumption

**SENT BY**
- Workplace Safety & Healthy (WSH) Office

**RECEIVED BY**
- All staff and vendors

**REMARKS**
Issued to all staff and vendors when return to premises is permitted

**MESSAGE BODY**
As the <type of incident> has been resolved, the organization will be taking steps to return to work premises.

With effect from <indicate date>, all staff and supporting vendors will resume business as usual operations, unless specified.

A follow up advisory will be sent shortly.

Check with your Managers for further clarification.

Thank you.

**MORE INFO LINKS / ATTACHMENTS**
<Insert link to internal BCP>

# Vulnerability – Indicators of Compromise (IOC) Notice

Scenario: Vulnerability Notification / IOC

Recommended Communications Guidelines:

- Obtain complete information pertaining to vulnerability prior to sending out messages
- Take note of any mandatory timeframe for implementation/execution (for example, for regulatory compliance).
- If you have an existing vulnerability procedure, do incorporate them in this template.

Note:

- The following are recommended messages to be sent as Alerts via BlackBerry Alert, based on the recommended frequency.
- Business leaders and dedicated coordinators are advised to revise/calibrate the message details in accordance to their endorsed response playbook and sector governance chapter (for example, the National Cyber Threat Response Center).
- An assumption is made in the provided template that the vulnerability notice or IOC is provided by a National Cyber Threat Response Center (NCTC), a regulatory authority or outsourced managed services agent. As an IT-security-related activity, response lead is undertaken by the SOC/IR/IT Security teams (where available).
- Unless otherwise specified, all responses shall be “(1) Acknowledged“ or “(2) I need further clarification“.

# 1. BlackBerry Alert Mobile App Registration

**PHASE**
- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**
- Immediate

**SENT BY**
- BlackBerry Alert Administrator

**RECEIVED BY**
- All Stakeholders who have yet to download the application

**REMARKS**
N/A

**MESSAGE BODY**
The BlackBerry Alert Mobile App can be downloaded onto your mobile device and used to receive notifications.

Follow the instructions attached to this email.

The Org Code is: (ORG CODE)

You will find the BlackBerry Alert Mobile app for iPhone:

https://apps.apple.com/us/app/blackberry-alert/id1551697059

You will find the BlackBerry Alert Mobile app for Android:

https://play.google.com/store/apps/details?id=com.blackberry.alert.prod

**MORE INFO LINKS / ATTACHMENTS**
N/A

## 2A. Assessment on Vulnerability / IOC

**PHASE**
- Response

**RECOMMENDED ISSUANCE AND FREQUENCY**
- When notified by NCTC, regulatory authority or engaged managed services agent

**SENT BY**
- Resilience office

**RECEIVED BY**
- SOC / Cyber / IT team

**REMARKS**
An assumption is made that the contact point with the local regulatory authority or managed services agent is the resilience office.

**MESSAGE BODY**
Dear SOC/IR/Cyber Response Team,

The attached vulnerability notice/IOC has been sent to us from the National Cyber Threat Response Center (NCTC)/Sector Regulator/Managed Services vendor for application XXX.

Action Required:

Please review the documentation and reply on the required measures to be taken via the attached LINK. Determine the relevant stakeholders to be informed and initiate via BlackBerry Alert.

**MORE INFO LINKS / ATTACHMENTS**
<Include links to vulnerability notice or IOC, relevant scenario playbook, assessment form, etc.>

## 2B. Action Required on Reported Vulnerability / IOC

**PHASE**
- Response

**RECOMMENDED ISSUANCE AND FREQUENCY**
- After review and assessment by the SOC, Incident Response (IR) team or mandated by sector regulator.

**SENT BY**
- SOC / Cyber / IT team

**RECEIVED BY**
- All impacted staff and vendors using the impacted application

**REMARKS**
N/A

**MESSAGE BODY**
Dear Recipient,

We have received the enclosed vulnerability/IOC Report impacting the listed applications.

Action Required:

a) <Input the required action expected, such as download latest version of application, or enable security updates to be conducted after office hours, etc.>.

b) Should you notice anything suspicious, immediately notify your supervisor and the security operations center.

c) Do not copy or forward the contents of this message to unauthorized recipients.

**MORE INFO LINKS / ATTACHMENTS**
<Include links to vulnerability notice or IOC, relevant scenario playbook, assessment form, etc.>

# IT Alerting

Scenario: Generic IT Incident Alerting

Recommended Communications Guidelines:

- Extract key details on the reported or escalated IT issue and provide the required SLA timeframe committed.
- Depending on the complexity of the reported IT issue, the proposed communication steps may need to be expanded or repeated until incident closure.
- If you have an existing response playbook/SOP, do incorporate them in this template.

Note:

- The following are recommended messages to be sent as Alerts via BlackBerry Alert, based on the recommended frequency.
- Business Leaders and dedicated coordinators are advised to revise/calibrate the message details in accordance to their endorsed response playbook.
- An assumption is made that relevant info is synchronized between public-facing online submission and the BlackBerry Alert application. Depending on classification of reported IT issue, relevant IT teams will be alerted for follow up resolution.
- Unless otherwise specified, all responses shall be “(1) Acknowledged and working on it“, “(2) I need further clarification“, or “(3) Action to be taken by re-assigned Team“.

# 1. BlackBerry Alert Mobile App Registration

**PHASE**
- Preparedness

**RECOMMENDED ISSUANCE AND FREQUENCY**
- Immediate

**SENT BY**
- BlackBerry Alert Administrator

**RECEIVED BY**
- All Stakeholders who have yet to download the application

**REMARKS**
N/A

**MESSAGE BODY**
The BlackBerry Alert Mobile App can be downloaded onto your mobile device and used to receive notifications.

Follow the instructions attached to this email.

The Org Code is: (ORG CODE)

You will find the BlackBerry Alert Mobile app for iPhone:

https://apps.apple.com/us/app/blackberry-alert/id1551697059

You will find the BlackBerry Alert Mobile app for Android:

https://play.google.com/store/apps/details?id=com.blackberry.alert.prod

**MORE INFO LINKS / ATTACHMENTS**
N/A

## 2. Notification of IT Service Issue (Incident Number XXX)

**PHASE**
- Response

**RECOMMENDED ISSUANCE AND FREQUENCY**
- Message is received after customer has completed online service request form

**SENT BY**
- BlackBerry Alert Administrator (or automated)

**RECEIVED BY**
- Relevant IT Response Team

**REMARKS**
Alert to be sent to relevant IT response team based on the category of IT incident reported. Alert to be pushed out manually, or automated where possible.

**MESSAGE BODY**
Dear IT Team,

The attached LINK contains a fault/service request just received.

Action Required:

Please review the service request and complete the service action form via the attached LINK. Should the request be performed by another team, reply accordingly.

**MORE INFO LINKS / ATTACHMENTS**
<Include links to service request form, relevant scenario playbook, appraisal form, etc.>

## 3. Completion of IT Service Issue (Incident Number XXX)

**PHASE**
- Recovery

**RECOMMENDED ISSUANCE AND FREQUENCY**
- Upon completion by relevant IT Response Team

**SENT BY**
- Relevant IT response team

**RECEIVED BY**
- IT response leader

**REMARKS**
Expected response will be “Acknowledged“ or “Need further clarification“.

**MESSAGE BODY**
Dear Recipient,

The reported IT issue has been resolved. The Incident Form has been completed via the following LINK.

Thank you.

**MORE INFO LINKS / ATTACHMENTS**
<Include links to completed service request form, etc.>