**“First 48” Response Plan (editable template)**

**Context:**

A cybersecurity or similar incident can have a significant impact on the business. The impact can be managed by a structured incident management process.

This process will initiate an appropriate response to an event which has the potential to cause significant damage to the company’s brand, reputation, customers and stakeholders.

In the event of this process being triggered it is essential that all stakeholders make themselves available for an initial emergency meeting or conference call as soon as possible, and are fully contactable throughout the process.

The first 24-48 hours are the most critical.

**Objective: to enable all parties to carry out their communications roles in a declared emergency and manage the incident to the end of the first impact phase.**

Contents

[Definitions 3](#_Toc70326554)

[First 48 Senior Group 4](#_Toc70326555)

[Dial in details for use by Senior Group only 5](#_Toc70326556)

[Communications Process 7](#_Toc70326557)

[Key Considerations 7](#_Toc70326558)

[Key Actions 7](#_Toc70326559)

[Emergency Room Calls 8](#_Toc70326560)

[Appendix A – Communications Guidelines 10](#_Toc70326561)

[Appendix B- Business Unit Incident Report 11](#_Toc70326562)

[Appendix C – Colleague and Customer Briefing 12](#_Toc70326563)

# Definitions

This document outlines the process designed to address any event, which has the potential to damage the Company brand and reputation and customers, damage shareholder confidence, or attract significant national press coverage. At this stage it may or may not be identified as a Cyber Attack so the Company’s standard incident response plan is deployed.

There are two primary categories of incident with associated levels of response. The processes outlined in this document apply to Category 1 incidents only. Certain incidents, could fall into either category. Examples of each include:

|  |
| --- |
| **CATEGORY 1 INCIDENT** Category 1 requires a First 48 response at Board level with considerations towards shareholders, the national press, customers, suppliers and colleagues.  |
| Leak or loss of confidential data including: * Confidential project or Company information not yet released
* Compromised financial transactions or monetary loss or risk of compromise
* Financial data/accounts prior to official release
* Customer data, customer account details

N.B. also may include GDPR data protection policy breach  |
| Major incident which affects day to day trading, such as: * Site or systems denial event due to a suspected Ransomware style attack
* Widespread systems crash or failure
* Significant Issue which prevents colleagues working for an extended period within systems or core processes
 |
| Customer or colleague death, or serious injury, whilst using company equipment, on company premises or involving a company vehicle or driver  |

|  |
| --- |
| **CATEGORY 2 INCIDENT** Category 2 classification of a less sever incident against the above criteria requires a scaled down response led by departmental Heads, Communications and Health & Safety or fraud teams, overseen by the CIO and Board as appropriate. |

# First 48 Senior Group

A senior management group (Senior Group) will be appointed to manage the incident on launch. This group will hold overall responsibility for decision making in relation to responses and work streams.

An **“Incident Manager”** will also be appointed at the outset and all communications will be channelled through this Manager.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Job Title**  | **Areas of Responsibility**  | **Deputy in Absence**  |
|  | CEO  | Group chair. Responsible for updating Chairman / PLC board.  |  |
|  | CFO  | Responsible for updating financial markets and shareholders.  |  |
|  | CCO  | Responsible for updating/liaising with suppliers, customers, Board, responsible for marketing and social media.  |  |
|  | HRD  | Responsible for all colleague and HR issues, internal communications and PR.  |  |
|  | CIO | Response for all systems and data related activities  |  |
|  | Company Secretary  | Legal advice.  |  |
|  | CSO  | Responsible for supplier interactions and related initiatives.  |  |

**Emergency Communications:**

# Dial in details for use by Senior Group only

Call number: xxx

International dial in: +xxx

Chairperson passcode: xxx then #

Participant passcode: xxx then #

These dial in details are strictly for use in First 48 scenarios. They should not be distributed or used for calls relating to any other projects.

NB: Voice and not data / video calling recommended to ensure the best coverage.

**Internal Stakeholders**

The contacts below are to be used as appropriate depending on the nature of the event taking place and the work streams required to respond.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name**  | **Job Title**   | **Areas of** **Responsibility**  | **Phone**  | **Email**  |
|  | Managing Director – Business 1  |  |  |  |
|  | Managing Director – Business 2  |  |  |  |
|  | Managing Director – Business 3  |  |  |  |
|  | Finance Director / Head of Finance |  |  |  |
|  | Communication Manager  |  |  |  |
|  | IT Director |  |  |  |
|  | E-Commerce |  |  |  |
|  |  Risk / Audit / Health & Safety |  |  |  |
|  | 3rd Parties |  |  |  |

**Out of Hours Numbers**

|  |  |  |
| --- | --- | --- |
| **Department**  | **Cover**  | **Number**  |
| IT SOC |  |  |
| Ecommerce  |  |  |
| Social mediaOther business processes |  |  |

# Communications Process

**INITIAL REPORTING**

* All risk related events should be reported up the line to the senior team, and by the senior team into a member of the Board. Any member of the Board can determine an event or incident a category 1, and trigger the First 48 process.
* As soon as this process is triggered, CEO will determine whether a call needs put into the Chairman to inform him of the incident and the First 48 process being triggered.

# Key Considerations

**Communications Scope**

When determining our response activities, all staff should be mindful that customers, suppliers and the press can contact COMPANY through a number of channels, all picked up by different colleagues and departments. Briefings for all relevant departments may include:

* Accounts/finance teams
* Call centres / subsidaries
* press@company.com email
* Recruitment team
* Social media channels
* Branches / outlets
* Account managers / Directors
* Procurement team

If there is potential for these colleagues to be contacted, brief them on how to handle these enquiries, give them a holding statement for response, and ask them to escalate any enquiries to their Manager.

**Customers Impacted?**

If there is large scale operational or customer related impact, or significant press coverage halt the following activity with immediate effect:

* Social media posting –respond to any queries (relating to general customer issues), but halt promotional content.
* Direct mail campaigns – any promotional or campaign based emails or letters should be halted.
* Outbound calling – all branches / outlets and head office teams should cease outbound calling activity to customers and prospects.
* Chat systems or other channels on COMPANY.com – if there is a risk this channel could be used for enquiries regarding this project, it should be suspended.

# Key Actions

Prior to the next meeting/call, ensure as much assessment and information as possible takes place, so an accurate picture of what has taken place is understood, why and how, and the current impact on the business. Each business unit or internal stakeholder will be responsible for gathering a report for their area for feedback to the Project Manager by close of play on day 1. An assessment template is shown in the appendix of this document. These reports should be collated by the Project Manager for feedback to the Senior Group by the end of the day.

All colleagues being briefed on the project should also be sent a copy of the communications guidelines in the appendix of this document. Depending on the nature of the issue they may also have to sign non-disclosure agreements.

# Emergency Room Calls

 **DAY 1, HOUR 1**

A meeting or call involving the Senior Group must take place as soon as possible after a category 1 issue occurring. The Process Manager will need to be briefed so they can begin to investigate the issue and its current impact on the business, as well as initiate the process by booking in the first call using the details below.

* Dial in details for conference call:
* Call number: xxx
* International dial in: +xxx
* Chairperson passcode: xxx
* Participant passcode: xxx
* Agenda:
* Run through and assessment of details available at this stage
* Analysis of current business impact (internally and externally), and potential for escalation
* Identification of key business functions affected  Identification of key external groups impacted:
	+ Customers o Suppliers o Shareholders
* Is there any press coverage at this stage, or likely to be?
* Agreement of initial response and messaging
* Identification and agreement of immediate actions, including:
	+ Internal stakeholders/business units to be briefed External stakeholders to be briefed
	+ External/internal statements required?
	+ Escalation to PLC Board, shareholders etc.
	+ Initiate external monitoring if required:
	+ Press
	+ City/financial press

**DAY 1, HOUR 3**

It is vital that no more than 3 hours passes between the kick off meeting and the second catch up. During this time, each business unit owner will be responsible for completing a thorough investigation and reporting back on the issue in progress, the current business impact and the potential for escalation. The Project Manager will collate and present the information from each area of the business back to the Senior Group.

**Agenda:**

* Review of information gathered by business unit owners
* Review of current business impact and potential for escalation
* Review of current activities to address issue
* Identification of next set of work streams and actions:
	+ Do we need an external statement ? – press, investor website etc.?
	+ Is there an impact on day to day operations? – this will require customer, colleague and supplier communication streams.
	+ Do we have a contingency action plan in place to ensure business continuity in affected areas?
* Determination of next levels of communication needed – Chairman, customers, press, colleagues etc.
* Colleague communication – if there is a large scale impact covered externally or which will affect customers it is vital we explain this to colleagues as early in the process as possible.

**END OF DAY 1**

The final call should take place at the end of day 1 to review all current responses, any escalation and the information gathered by each business unit, especially relating to colleague and customer feedback, and any press coverage.

Agenda

* Review any further information or escalation from business unit owners.
* Review any press coverage, colleague queries or concerns raised.
* Review any enquiries from customers, suppliers, shareholders etc.
* Determination of next steps.
* Plan for Day 2

**Day 2**

* Implement communications plan and actions determined at close of Day 1

# Appendix A – Communications Guidelines

These guidelines are for any COMPANY colleagues being briefed on the project.

All communications between colleagues, or with external suppliers or partners in relation to this project are strictly private and confidential. Depending on the nature of the issue, colleagues or external partners may be asked to sign Non-Disclosure Agreements prior to joining the project group. All colleagues and external partners briefed on the issue or event must be recorded in the template below, and must report directly into the Incident Manager.

|  |  |  |
| --- | --- | --- |
| **Colleague Name**  | **Business Unit**  | **Date of Briefing**  |
|   |   |   |
|   |   |   |
|   |   |   |

Any business unit owner briefed on the issue or event should only cascade this information to colleagues within their teams or other areas of COMPANY with the express permission of the Senior Group.

When communicating about any aspect of this issue or event emails should be sent with the subject line “First 48”. All information should be within an Office document, not the body of an email. All documents should be password protected, and passwords sent via text to the recipient.

Any phone calls made regarding aspects of the incident t should be completed in private meeting rooms in COMPANY locations, or in public areas where they are unlikely to be overheard.

# Appendix B- Business Unit Incident Report

This template should be used by any business unit asked to assess and report back on their area by the Senior Group on day 1. All completed reports should be sent back to the Incident Manager.

|  |  |
| --- | --- |
| **Name**  |   |
| **Business unit**  |   |
| **Areas of responsibility**  |   |
| **Assessment of current impact on these functions**  |   |
| **Any relevant feedback from third parties (customers, press, suppliers etc.)**  |   |
| **Any relevant feedback from colleagues**  |   |
| **Your assessment of potential for escalation of this impact**  |   |
| **Suggested response or next steps for addressing in your area**  |   |

# Appendix C – Colleague and Customer Briefing

This document is designed to brief COMPANY colleagues in roles which place them in a position where they are likely to be contacted by external parties in relation to this project.

**OVERVIEW**

We are currently in a position as a business where you may be contacted by customers, suppliers, members of the press, or other external parties in relation to xxxxx. We understand this can be difficult, which is why we’ve put together the statements below for you to use in response. It is incredibly important that you stick to these and don’t enter into a discussion, or give them any additional information about COMPANY or what is going on. If they try to push you, simply tell them that is all the information you have at this time, but you will forward their query and contact details and someone will come back to them.

You should record the questions that they ask you, their name and contact details, and any other information they provide. You should then forward this through to the Project Manager (TBC).

**STATEMENT FOR CALLS OR EMAILS**

Thank you for contacting us. This is the xxxx department, so I’m afraid we can’t give you any information about xxxx. I believe the issue in question is currently being investigated, but if you leave your details with me I can ask one of our communications team to come back to you as soon as they can.

**STATEMENT FOR SOCIAL MEDIA**

Please email press@company.com and someone will come back to you. Thank you.

**Internal Statement - template**

This is an initial statement for release to staff in the event the issue has garnered national / international media attention which it is likely they will have seen. This should be emailed to all Group colleagues and uploaded to the homepage of COMPANY Intranet.

XXX

**External Statement**

* Marketing Department or Press Office should prepare appropriate announcements in conjunction with Senior Group. No other communication should be issued.