|  |
| --- |
| [Company name] |
| Incident Response Plan Template |
|  |

|  |
| --- |
| Name[Date] |



Table of Contents

[1.0 - Executive Support 4](#_Toc85976114)

[2.0 - Process Description 4](#_Toc85976115)

[3.0 - Incident Priority Levels and Restoration Times by Criticality Level 5](#_Toc85976116)

[4.0 - Plan Activation Criteria 6](#_Toc85976117)

[5.0 - Assignment of Responsibility 6](#_Toc85976118)

[6.0 - Communication Channels 7](#_Toc85976119)

[7.0 - Key Contacts 8](#_Toc85976120)

[8.0 - Service Owner(s) 9](#_Toc85976121)

[9.0 - Essential Roles and Alternates 9](#_Toc85976122)

[10.0 - Essential Information Assets 10](#_Toc85976123)

[10.1 - IR Considerations for Information Assets 10](#_Toc85976124)

[11.0 - Essential Technology Assets 11](#_Toc85976125)

[12.0 - Primary and Alternate Site(s) 12](#_Toc85976126)

[13.0 – Plans of Action 13](#_Toc85976127)

[14.0 – Testing Schedule for this Plan 13](#_Toc85976128)

[15.0 – Supporting and Related Plans 14](#_Toc85976129)

**Disclaimer***The information provided by M3 Networks Limited, trading as HighGround (“we”, “us” or “our”) on and originating from highground.io (and on our mobile applications) is for general use purposes only. We shall not be liable for any loss of profits or revenues, whether incurred directly or indirectly, damages incurred, or any loss of data, use, goodwill, reputation, or other intangible losses, resulting from the use of this document. All information and content is provided in good faith, however we make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, reliability, availability or completeness, free from viruses or malicious code, of any information or content on or originating from highground.io (or our mobile applications). It is the sole responsibility of the consumer of any information or content to ensure its suitability for use*.

**Document Control**

|  |  |
| --- | --- |
| **Organization** | Organization Name |
| **Title** | Incident Response Plan |
| **Revision** | V3 – 09/10/21 |
| **Author** | Author Name |
| **Owner** | Document Owner |
| **Classification** | Confidential – Authorized Personnel Only |
| **Review date** | Next Review Date |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Inc. Date** | **Author** | **Previous Version** | **Purpose and Summary of Revision** |
| *V1 – 01/01/21* | *Author Name* | *N/A* | *Original Version* |
| *V2 – 04/05/21* | *Author Name* | *V2* | *Semi-Annual Scheduled Review* |
| *V3 – 09/10/21* | *Author Name* | *V3* | *Change in Executive Leadership* |

**Document Approvals**

This document requires approval, and has been approved by the following executives:

|  |  |  |
| --- | --- | --- |
| **Position** | **Name** | **Date** |
| *CEO* | *Barack Obama* | *09/10/2021* |
| *CFO* | *Rishi Sunak* | *09/10/2021* |
| *COO* | *Boris Johnson* | *09/10/2021* |
| *CTO* | *Bill Gates* | *09/10/2021* |

**Document Distribution**

This document should be distributed to:

|  |  |  |
| --- | --- | --- |
| **Name** | **Job Title** | **Email Address** |
| Board of Directors | N/A | <enter email addresses> |
| Heads of Department | N/A | <enter email addresses> |
| HighGround Incident Response Operations Centre | Incident Response Handlers | incidentresponse@highground.io  |

**Contributors**

The following individuals and organizations have contributed to the development of this Incident Response Plan:

|  |  |  |
| --- | --- | --- |
| **Individual or Organization Name** | **Email Address** | **Contact Number** |
| CEO | <enter email address> | <enter Tel#> |
| HighGround Professional Services Team | <enter email address> | <enter Tel#> |

# 1.0 - Executive Support

*[List executives who had input to this document and have approved its development, applicability and suitability for use in the organization]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Name of Executive** | **Position** | **Date** | **Signature** |
| *Barack Obama* | *CEO* |  *01/05/2021* |  |
| *Boris Johnson* | *COO* |  *01/05/2021* |  |
|  *Rishi Sunak* | *CFO* |  *01/05/2021* |  |
|  *Bill Gates* | *CTO* |  *01/05/2021* |  |

# 2.0 - Process Description

*[Provide a high-level overview if your incident management process to aid an incident response handler implementing this IR Plan.]*

|  |
| --- |
| *[Example: Incident Response and Management is outlined to HighGround Incident Response Operations Centre. The process is as follows:* 1. *Incident Recording & Assignment*
2. *Incident Triage*
3. *Incident Notification*
4. *Incident Containment & Evidence Gathering*
5. *Incident Eradication*
6. *Incident Recovery*
7. *Incident Documentation & Impact Assessment*
8. *Post Incident Analysis*
9. *Incident Reporting & Disclosure]*

 |

# 3.0 - Incident Priority Levels and Restoration Times by Criticality Level

*[Detail the Priority Levels and Restoration Times of cyber and information security incidents by impact and criticality level]

[Example table below – aligned with HighGround Incident Response Operations Centre]*

|  |  |
| --- | --- |
| ***Priority Level*** | ***Service Restoration Time Objective*** |
| *P1* | ***Grade:*** *Severe****RTO:*** *1 hours or less, within same day as reported****Description:*** *Affects mission critical data and resources, and results in severe business and financial losses* |
| *P2* | ***Grade:*** *Major****RTO:*** *2 hours or less, within same day as reported****Description:*** *Affects highly sensitive data and resources to impact business functionality* |
| *P3* | ***Grade:*** *High****RTO:*** *4 hours or less, within same day as reported****Description****: Affects systems, functions and services containing small amounts of sensitive data* |
| *P4* | ***Grade:*** *Moderate****RTO:*** *8 hours or less* ***Description****: Impacts marginal number of systems holding moderate sensitive information, malicious code, Unauthorized Access Attempts/Requests* |
| *P5*  | ***Grade:*** *Low****RTO:*** *1 to 2 working days****Description****: Impacts information systems holding basic information, Inappropriate Usage such as violating computer use policies* |
| *P6* | ***Grade:*** *Irrelevant****RTO:*** *1 to 2 working days****Description****: Incident shows negligible impact on the system or poses no damage to reputation* |
| *P7* | ***Grade:*** *Exercise / Network Defense Training****RTO:*** *N/A****Description****: Used for authorized training exercises and is not applicable* |

# 4.0 - Plan Activation Criteria

*[What conditions must be met before the incident response plan can be executed]*

|  |
| --- |
| *[Example: A HighGround Incident Response Handler must have completed Incident Triage and confirmed the reported cyber security incident is a Verified Cyber Security Incident]* |

# 5.0 - Assignment of Responsibility

*[List employees in your organization who are responsible for developing and maintaining this Incident Response plan]*

*[Example table below]*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Position** | **Date Assigned** | **Responsibility** | **Signature** |
|  *Barack Obama* | *CEO* |  *01/05/2021* | *Sponsor* |  |
|  *Boris Johnson* | *COO* |  *01/05/2021* | *Owner, Review & Maintain* |  |
|  *Rishi Sunak* | *CFO* |  *01/05/2021* | *Review and Contributor* |  |
|  *Bill Gates* | *CTO* |  *01/05/2021* | *Review and Contributor* |  |

**For the rest of the Incident Response Plan please sign up for free at** [**highground.io**](https://portal.highground.io/sign-up) **and navigate to the compliance manager where you will find free guides to Incident Response and other Compliance needs.**