

Hub88 International B.V.

**Information Security Policy
v.1.0**



1. Version control

Document Status

Version Number	v.1.0
Status	Active
Approving Official	Gabriel Kolawole
Responsible Office	Product & Engineering

Version Control

Effective date	Version	Comments	Subsequent Review Date
02.01.2026	v. 1.0	Initial Release	02.01.2027

2.Contents

1. Version control.....	2
2. Contents	3
3. Introduction	4
4. Incident Response Flowchart.....	6
5. Incident Detection and Analysis	7
5.1. Impact Assessment	7
5.2. Incident Prioritization	8
6. Activating the Incident Response Procedure.....	9
7. Assemble Incident Response Team	10
Incident Response Team Members Roles and Responsibilities	10
8. Incident Containment, Eradication, Recovery and Notification	12
a. Containment.....	12
b. Eradication	13
c. Recovery.....	14
d. Notification	14
9. Post-Incident Activity.....	15

3. Introduction

This document defines the information security policy of Hub88 International B.V.

As a modern, forward-looking business, Hub88 International B.V. recognizes the need to ensure its operations run smoothly and without interruption to benefit customers, shareholders, and stakeholders.

This policy applies to all systems, people, and processes that constitute the organization's information systems, including board members, employees, suppliers, and relevant third parties who access Hub88 International B.V. systems. Senior Management is responsible for its implementation and enforcement.

Access to systems and data is granted using least privilege principles with strong passwords and multi-factor authentication required. Sensitive data, including customer and business information, must be encrypted both during transmission and at rest. It must be stored, processed, and transmitted securely to prevent unauthorized access. Security incidents must be reported immediately to the Physical & Cyber Security Team.

Security guidelines and updates promoting best practices and addressing emerging threats will be provided to all employees.

Access to facilities and critical infrastructure is restricted to authorized personnel, with surveillance and monitoring systems ensuring physical security. Security controls will be integrated into IT operations, including software updates, system monitoring, and incident management. To ensure their effectiveness, security controls testing should be implemented continuously as part of these processes. Regular backups will ensure data recovery during disruptions.

Hub88 International B.V. uses data centers that comply with international standards and have been tested for information security and integrity by an independent qualified entity.

Hub88 International B.V. shall be responsible for regular maintenance of the equipment and software, it shall replace or expand it as necessary to ensure the integrity of the operation.

Violations of this policy may result in disciplinary actions, up to and including termination of employment or contracts.

This policy shall also be used when an incident of some kind has occurred that affects the security of Hub88 International B.V. It is intended to ensure a quick, effective and orderly response to information security incidents.

The procedures set out in this policy should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding the actions to take.

However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this response procedure are to:

- Provide a concise overview of how Hub88 International B.V. will respond to an incident affecting its information security
- Set out who will respond to an incident, and their roles and responsibilities
- Define how decisions will be taken regarding our response to an incident
- Explain how communication within the organization and with external parties will be handled
- Provide contact details for key people and external agencies
- Define what will happen once the incident is resolved, and the responders are stood down

All personal information collected as part of the incident response procedure set in this policy will be used purely for the purposes of information security incident management and is subject to relevant data protection legislation.

This policy should be reviewed within one year, with subsequent reviews occurring once every three years.

4. Incident Response Flowchart

The flow of the incident response procedure is shown in the diagram below.

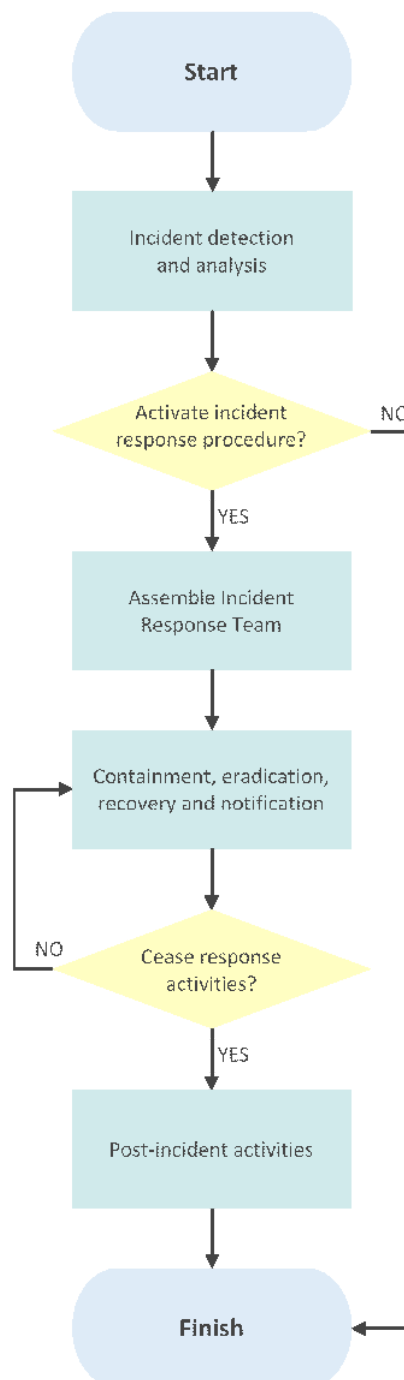


Figure 1 – Incident response flowchart

These steps are explained in more detail in the rest of this procedure.

5. Incident Detection and Analysis

The incident may be initially detected in a wide variety of ways and through a number of different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within Hub88 International B.V. or by employees noticing unusual activity. Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because the stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

5.1. Impact Assessment

Once the incident has been detected, an initial impact assessment must be carried out in order to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation
- The information assets that may be at risk or have been compromised
- The likely duration of the incident, i.e. when it may have begun
- The business units affected and the extent of the impact to them
- Initial indication of the likely cause of the incident

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets, business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

5.2. Incident Prioritization

Based on the impact assessment, an incident will be assigned a priority of P1, P2 or P3. The guidance in the table below will be used in deciding priority.

PRIORITY	DESCRIPTION
P1	- One or more systems are compromised, infected with malware. Our internal system is being attacked and is unable to function - Business Web Application is not functioning due to compromise or attack
P2	- Internal data/system has been compromised and there is no active ongoing attack - Compromises involving financial crimes - Larger scale account take-over and unauthorized access to customer accounts (>100 accounts)
P3	- Attempt to compromise Hub88 International B.V. system by external actor - User account take-over and unauthorized access to customer accounts (<100 accounts)

Table 1: Incident priorities

6.Activating the Incident Response Procedure

Once notified of an incident, the Incident Management Team must decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response Procedure and the convening of the Incident Response Team (IRT).

Guidelines for whether a formal incident response should be initiated for any particular incident of which the Incident Management Team has been notified are if any of the following apply:

- There is significant actual or potential loss of classified information
- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may cause significant impact on the organization

In the event of disagreement or uncertainty about whether or not to activate an incident response the decision of the Incident Management Team will be final.

If it is decided not to activate the procedure, then a plan should be created to allow for a lower-level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.

If the incident warrants the activation of the IR procedure the Incident Management Team will start to assemble the IRT.

7. Assemble Incident Response Team

Once the decision has been made to activate the incident response procedure, the Incident Management Team will ensure that all role holders are contacted, made aware of the nature of the incident and asked to assemble at an appropriate location (if applicable).

Incident Response Team Members Roles and Responsibilities

The responsibilities of the roles within the incident response team are as follows:

Incident Management Team

- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement
- Overall coordination of the incident response team
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status in Slack
- Facilitates communication via Slack, telephone or other methods
- Assesses the extent and impact of the incident together with the other stakeholders/response teams involved
- Liaises with the IRT on an on-going basis to provide updates and answer any questions required for decision-making by the IRT or involves the relevant parties who can answer

Information Technology

- Provides input on technology-related issues
- Assists with impact assessment

Business Operations

- Contributes to decision-making based on knowledge of business operations,

products and services

- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the organization

Facilities Management

- Deals with aspects of physical security and access
- Provides security presence if required

Human Resources

- Assesses and advises on HR policy and employment contract matters
- Represents the interests of organisation employees
- Advises on capability and disciplinary issues

Communications (PR and Media Relations)

- Responsible for ensuring internal communications are effective
- Decides the level, frequency and content of communications with external parties such as the media
- Defines approach to keeping affected parties informed e.g. customers, shareholders

Legal and Compliance

- Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks
- Assesses the actual and potential legal implications of the incident and subsequent actions

8. Incident Containment, Eradication, Recovery and Notification

This section describes the main steps involved in managing an incident. Additional procedures and plans are available to cover the specifics of these steps for particular types of incidents, for example ransomware, denial of service and data breach.

a. Containment

The first step will be to try to stop the incident getting any worse i.e. contain it. In the case of a virus outbreak this may entail disconnecting the affected parts of the network; for a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Principle 1 – Don't change any data. If anything is done that results in the data on the relevant system being altered in any way then this will affect any subsequent court case.

Principle 2 – Only access the original data in exceptional circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g. time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.

Principle 3 – Always keep an audit trail of what has been done. Forensic tools will do this automatically but this also applies to the first people on the scene. Taking photographs and videos is encouraged as long as nothing is touched to do it.

Principle 4 – The person in charge must ensure that the guidelines are followed.

Prior to the arrival of a specialist basic information should be collected. This may include:

- Photographs or videos of relevant messages or information
- Manual written records of the chronology of the incident
- Original documents, including records of who found them, where and when
- Details of any witnesses

Once collected, the evidence will be kept in a safe place where it cannot be tampered with and a formal chain of custody established.

The evidence may be required:

- For later analysis as to the cause of the incident
- As forensic evidence for criminal or civil court proceedings
- In support of any compensation negotiations with software or service suppliers

Next, a clear picture of what has happened needs to be established. The extent of the incident and the knock-on implications should be ascertained before any kind of containment action can be taken.

Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

b. Eradication

Actions to fix the damage caused by the incident, such as deleting malware, must be put through the change management process (as an emergency change if necessary). These actions should be aimed at fixing the current cause and preventing the incident from reoccurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

c. Recovery

During the recovery stage, systems should be restored back to their pre-incident condition, although necessary actions should then be performed to address any vulnerabilities that were exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers and amending procedures.

d. Notification

The notification of an information security incident and resulting loss of data is a sensitive issue that must be handled carefully and with full Senior Management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take.

Hub88 International B.V. will always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident, such as credit monitoring services.

Records collected as part of the incident response may be required as part of any resulting investigations by relevant regulatory bodies and Hub88 International B.V. will cooperate in full of such proceedings.

Hub88 International B.V. will provide the Curaçao Gaming Authority (CGA) with all information and reports that the CGA considers necessary for monitoring compliance with the provisions of or pursuant to the law.

The reports include at least:

- a. A change report.
- b. An incident report – The incident report shall be submitted to the CGA within 24 hours after an incident.
- c. A report prepared by an independent expert, assessing the license holder's compliance with system configuration requirements – The report shall be provided periodically to the

CGA upon request.

The CGA may provide a template for the reports, which should be checked on the CGA's website.

In the incident reports, Hub88 International B.V. shall at a minimum report on the following issues, where applicable to its business model:

- a) any gaming security breaches that (may) have compromised personal information of gamblers or game details, along with measures taken in response.
- b) failure or loss of, or damage to, all or part of the equipment or software that (may have) resulted in the loss of all or part of the Remote Games of Chance offered, along with measures taken in response.
- c) gaming-related (attempted) fraud or other forms of criminal behavior of players, along with measures taken in response.
- d) any other behaviors or events that may pose a serious threat to the responsible, reliable, and verifiable organization of the Games of Chance offered, or that may undermine the public trust in the responsible, reliable, and verifiable organization of the licensed Games of Chance.

9. Post-Incident Activity

The Incident Management Team will decide, based on the latest information from other members of the team, the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of plans may continue beyond this point but under less formal management control.

This decision will be up to the Incident Management Team's judgement but should be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable
- The pace of change of the situation has slowed to a point where few decisions are required
- The appropriate response is well underway and recovery plans are progressing to schedule

- The degree of risk to the business has lessened to an acceptable point
- Immediate legal and regulatory responsibilities have been fulfilled

If recovery from the incident is on-going the Incident Management Team should define the next actions to be taken. These may include:

- Informing all involved parties that the IRT is standing down
- Ensuring that all documentation of the incident is secured
- Requesting that all staff not involved in further work to return to normal duties

Any immediate comments or feedback from the team will be recorded. A more formal post-incident review will be held at a time to be decided depending to the magnitude and nature of the incident.