

Hub88 International B.V.

Curaçao



Information Security Policy

v. 2.0

1. Version Control

Document Status

Version Number	V 2.0
Status	Active
Approving Official	Gabriel Kolawole
Authorization and approved by	The Directors of Hub88

Version Control

Effective date	Version	Author	Comments
01.01.2026	v. 1.0	Gabriel Kolawole	Initial Release
01/07/2026	v.2.0	Gabriel Kolawole	Revision to align with applicable information security control requirements for CGA licensees. Addition of Section 11 (Information Security Controls) Updated to new Hub88 Policy Format

Policy Review Log

Review date	Reviewer	Comments /Actions taken
01/10/2026		

2. Contents

1.	Version Control	2
2.	Contents.....	3
3.	Definitions.....	4
4.	Introduction	5
5.	Incident Response Flowchart.....	6
6.	Incident Detection and Analysis	7
6.1	Impact Assessment	7
6.2	Incident Prioritisation.....	7
7.	Activating and the Incident Response Procedure	8
8.	Assembling the Incident Response Team.....	8
9.	Incident Containment, Eradication, Recovery and Notification	10
9.1	Containment	10
9.2	Eradication	11
9.3	Recovery	11
9.4	Notification	11
10.	Post-Incident Activity	12
11.	Information Security Controls	12
11.1	Account, Administrator and Privileged Account Management	13
11.2	Vulnerability and Patch Management	14
11.3	Security Awareness and Training.....	15
11.4	Data Masking and Non-Production Environments.....	16
11.5	Third-Party Management and Data Feed Integrity	17
11.6	Logging and Monitoring	19
11.7	Malware Defence and Removable Media.....	20
11.8	Backup and Data Recovery	21
11.9	Business Continuity and Operational Resilience.....	21
11.10	Asset Management	22

11.11	Data Classification and Protection	23
11.12	Secure Configuration.....	24
11.13	Access Control and Authentication	25
11.14	Web and Email Protection.....	26
11.15	Network Infrastructure Security.....	26
11.16	Physical and Environmental Security.....	27
11.17	Human Resource Security	27
11.18	Legal and Regulatory Compliance	29
11.19	Cryptographic Controls and Key Management	29
11.20	Security Governance and Compliance Assurance	30
11.21	Incident Response Timeframes, Escalation and Notification	31

3. Definitions

Hub88	Means Hub88 International B.V.
The Code	Code of Business Conduct
Employees	Employees, officers and directors of Hub88's Employment Entities
Other representatives	Contractors, agents, consultants and other representatives of Hub88 and its subsidiaries
IR	Incident Response
IRT	Incident Response Team
CGA	Curaçao Gaming Authority
ISO	Information Organisation of Standardisation
ISMS	Information Security Management System
CIS	Centre for Internet Security
IG1	Implementation Group 1
AWS	Amazon Web Server
IAM	Identity and Access Management
CVSS	Common Vulnerability Scoring System
SSL	Secure Sockets Layer
TLS	Transport Layer Security
SSH	Secure Shell
PGP	Pretty Good Privacy
GPG	GNU Privacy Guard
API	Application Programming Interface
RSA-SHA256	Hashing Algorithm that combines the SHA-256 and RSA Public Key Encryption
CEO	Chief Executive Officer
CTO	Chief Technical Officer
COO	Chief Operations Officer
CO	Compliance Officer

4. Introduction

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

As a modern, forward-looking business, Hub88 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 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 uses data centres that comply with international standards and have been tested for information security and integrity by an independent qualified entity.

Hub88 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. 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 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 is reviewed quarterly.

5. Incident Response Flowchart

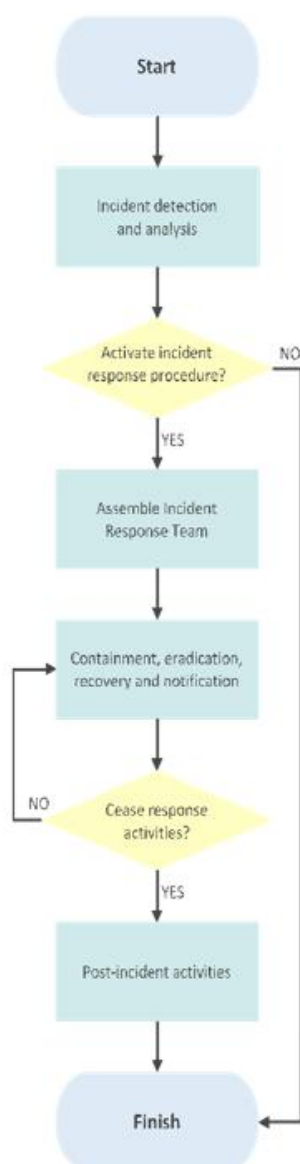


Figure 1 – Incident Response Flowchart

These steps are explained in more detail throughout this procedure

6. 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 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.

6.1 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.

6.2 Incident Prioritisation

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 Hub88s' system by external actor • User account take-over and unauthorized access to customer accounts (<100 accounts)

Table 1: Incident Priorities

7. Activating and 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.

8. Assembling the 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

9. 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.

9.1 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.

9.2 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.

9.3 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.

9.4 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 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 will cooperate in full of such proceedings. Hub88 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.

At minimum, the reports must include:

- 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 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 behaviour of players, along with measures taken in response.
- d) any other behaviours 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.

10. 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 in 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 parties involved that the IRT is standing down
- Ensuring that all documentation of the incident is secured
- Requesting that all staff that are not involved in further work 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 on the magnitude and nature of the incident.

11. Information Security Controls

This section sets out the foundational information security controls applied by Hub88. These controls are based on the Centre for Internet Security (CIS) Controls Implementation Group 1 (IG1) and are mapped where applicable to ISO/IEC 27001:2022.

Hub88 is licensed as a Business-to-Business gaming technology provider and is subject to these requirements in its own right. Where a control is delivered in whole or in part through a Hub88 Group policy, that policy applies in addition to this one.

11.1 Account, Administrator and Privileged Account Management

Accounts, standard, administrative, and service are inventoried, provisioned under least privilege principles, and deactivated promptly when they are no longer required. Access is granted through a documented provisioning process requiring management approval and is revoked immediately upon termination of employment or change of role.

Accounts that remain enabled but unused present a particular risk, as they are unlikely to be monitored and their misuse is unlikely to be noticed or reported. Hub88 therefore applies the following control:

- Standard user accounts with no authentication activity for 45 consecutive days are disabled. Accounts are disabled rather than deleted, so that audit history and attribution are preserved. Reactivation requires a request through the normal access provisioning process, with management approval, and is recorded.

Enforcement is through Hub88's identity provider, Keycloak, federated with Google single sign-on. Login-event retention is configured to exceed forty-five days so that inactivity can be measured reliably, and federated sign-on events are recorded as login events. Accounts are additionally removed through the joiner, mover and leaver process and confirmed at each quarterly access review.

Accounts held outside the identity provider, including AWS IAM users, direct database accounts, and non-federated tooling, are not subject to automated inactivity disablement. These accounts are governed instead by the following controls, which apply in combination:

- **Revocation on departure** - All such accounts are disabled as part of the joiner, mover and leaver process when an individual leaves Hub88 or changes role.

Continued business need, ownership, and appropriate privilege level are confirmed at each access review cycle. Access reviews are conducted quarterly and are carried out by the security function.

- **Network-level access restriction** - Database access and the majority of database-adjacent administrative access are reachable only through Hub88's VPN. These credentials are therefore not exposed to the public internet and cannot be exercised without prior authenticated network access.
- **Privilege separation on data stores** - Direct write access to production databases is restricted to the Database Administrator role. All other database access is read-only, with data modification in production occurring through the application layer and Hub88's change management process rather than by direct database operation.

Non-interactive service, system, and integration accounts are exempt from automated inactivity disablement, as legitimate operational patterns such as scheduled or low-frequency batch processes may produce extended periods without authentication. Such accounts are subject instead to documented periodic review confirming continued business need and appropriate ownership. Each exempt account has a recorded owner and justification.

Non-interactive service, system, and integration accounts are confirmed as exempt from automated inactivity disablement. Each exempt account has a recorded owner and justification and is subject to review of continued business need at each quarterly access review.

11.2 Vulnerability and Patch Management

Hub88 recognizes that container vulnerabilities are frequently resolved upstream, through a patched base image published by the image maintainer, and that the timing of such fixes is not always within its direct control. This policy therefore establishes defined timeframes for the actions Hub88 does control — the triage of findings, and remediation once a fix is available — together with documented and actively managed risk acceptance where no upstream fix yet exists. The objective is not the absence of all vulnerabilities at build time, but that no identified vulnerability remains untracked or without a conscious remediation or risk acceptance decision.

Detection covers vulnerable operating system packages and application dependencies within container images. Dependencies bundled into a built image are enumerated by the image scan.

Amazon GuardDuty is deployed and provides continuous threat detection across the environment, analysing management-plane activity, network flow, and name resolution telemetry for indications of malicious or anomalous behaviour. GuardDuty is a threat detection service and does not perform vulnerability scanning of deployed workloads; it is complementary to, and not a substitute for, the workload scanning described below.

Scanning coverage therefore comprises detection of vulnerable operating system packages and application dependencies within container images, applied at build and repeated on the cycle described below, together with continuous runtime threat detection across the cloud environment.

Triage and remediation.

Vulnerabilities are triaged by severity using the CVSS rating emitted by the scanning tool. Two timeframes apply. The first is the maximum period to review a finding and decide an action, being either remediation or formal risk acceptance; this is within Hub88's control and applies in all cases. The second is the maximum period to rebuild and deploy once a fix becomes available.

SEVERITY	TRIAGE WITHIN	REMEDiate WITHIN (FROM FIX AVAILABILITY)
Critical	7 days	15 days
High	14 days	45 days
Medium	30 days	90 days
Low	Best effort	Next release cycle

Table 2: Vulnerability triage and remediation timeframes

Critical and High severity findings are addressed within the timeframes above. Medium and Low severity findings are addressed through the quarterly technical debt cycle.

The triage period is shorter than the remediation period because triage requires only that a finding be reviewed and a decision recorded, which is entirely within Hub88s' control. The remediation period begins only once a fix is available and allows for the rebuilding of affected images, regression validation across dependent services, and deployment through the change management process.

Findings for which no upstream fix is available.

Where no upstream fix has been released, the finding is recorded as a documented risk acceptance stating the rationale, any compensating controls in place such as network isolation or restricted exposure, and owner sign-off. Such findings are re-reviewed at each monthly cycle and moved to remediation as soon as a fix is released. No finding is closed or dismissed solely because an immediate fix is unavailable.

All Critical and High severity findings are recorded in a tracking workflow with the assigned owner, severity, status, and due date aligned to the timeframes above.

Base images are scanned on every build, and currency is addressed through the build and remediation cycle rather than through a separate periodic review.

Images that have not been rebuilt are rescanned on a quarterly cycle, so that vulnerabilities disclosed after an image was last built are identified for components that remain in service without redeployment. Findings from such rescans are triaged and remediated under the timeframes set out above.

Patching is remediation-driven rather than calendar-driven. Updates are applied and shipped to production as remediation is completed under the timeframes above, rather than on a fixed monthly schedule.

Patch application.

Patches are incorporated when images are built and are applied to production as remediation is completed under the severity-based timeframes set out above. This remediation-driven approach is adopted in place of a fixed monthly patching schedule and is supported by the following controls:

- Vulnerability scanning is performed on every build rather than periodically
- Images not rebuilt within the period are re-scanned quarterly
- Remediation is bound by defined triage and remediation timeframes by severity.

The approach is reviewed at each annual review of this programme. Penetration testing is performed annually and additionally following significant architectural change. Findings are triaged and tracked to closure under the same model as scanning findings.

Programme governance.

Tooling coverage, triage and remediation timeframes, base image currency, and the risk acceptance backlog are reviewed at least annually, or following significant change to the environment or to the threat landscape. Timeframes are expected to tighten as the process matures, consistent with progression toward CIS Implementation Group 2.

11.3 Security Awareness and Training

All personnel receive security awareness training at onboarding and annually thereafter, supplemented by role-specific training for functions carrying elevated information security risk.

An annual training cadence and programme ownership are established. The Data Privacy Team provides annual training to all employees, in accordance with the Hub88 Group Data Protection Policy v1.0, section 9.5.

The annual cycle covers data protection and awareness of data protection law, together with information security awareness comprising recognition of phishing and social engineering, credential and authentication hygiene, secure use of systems and assets, and the detection and reporting of incidents.

Personnel in roles with elevated risk exposure receive additional targeted training as follows:

- **Engineering** - Secure development practices, dependency and patch hygiene, and the detection and escalation of incidents.
- **Core Platform and infrastructure** - Privileged access management, authentication controls, and secure remote access.
- **Finance and operations** - Social engineering, business email compromise, and payment fraud awareness.
- **Personnel handling operator or transaction data** - Data classification and handling, secure transfer, and the prevention of accidental disclosure.

Training content addresses aggregation-layer risks specific to Hub88, such as API abuse and credential stuffing against operator integrations, alongside general phishing and social engineering awareness.

Training completion is recorded for each individual and retained as evidence of compliance, available for regulatory inspection and internal audit.

Training completion is recorded on the Staff Training Register maintained by the Compliance Officer. Delivery of the training cycle is supported by a third-party training provider.

The Hub88 Group policies apply to Hub88 Limited and Hub88 International B.V. collectively.

11.4 Data Masking and Non-Production Environments

Production data is not used in Hub88s' non-production environments. Functional testing by development and quality assurance, and regression testing in the staging environment, are performed exclusively against purpose-created test data. The copying, exporting, or restoring of production data into any non-production environment is not permitted.

Because no production data is replicated into these environments, the exposure that data masking is intended to mitigate — the presence of regulated data in environments subject to weaker access control and monitoring than production — does not arise. Where production-like data characteristics are required for testing, representative test data is generated rather than derived from production records.

Hub88 does not collect personal data from players. Player identity data is held by the operator, and the platform processes pseudonymous identifiers and transaction records. This further limits the categories of regulated data that could be exposed through non-production use.

Should any future requirement arise to use production-derived data outside the production environment, including for analytics or diagnostic purposes, such data must be masked or anonymised before use, and the exception must be documented and approved.

Analytics and reporting queries are served from a production replica and from a data warehouse, both of which reside within the production environment. Non-production environments replicate the same architecture but contain no production data.

11.5 Third-Party Management and Data Feed Integrity

Hub88 operates as an aggregation platform, receiving game content, results, and transaction data from licensed B2B suppliers and making that content available to operators. Hub88 therefore occupies both sides of the third-party integrity relationship: it consumes externally supplied data, and it supplies data onward. The controls in this section address the authenticity, integrity, and continued reliability of that data.

Contractual delegation of operational controls to a supplier does not relieve Hub88 of its regulatory accountability under the LOK.

Source authentication and integrity validation. All platform API traffic is exchanged over authenticated and encrypted channels. Every request carries a cryptographic signature generated using RSA-SHA256, validated against the counterparty's registered public key, with a distinct key pair maintained per operator integration. A request whose signature does not validate is rejected. This provides assurance both that a message originates from the registered counterparty and that its content has not been altered in transit.

Signature validation establishes authenticity and integrity in transit. It does not, by itself, establish that the content of a validly signed message is correct. A supplier whose own systems are compromised, whose signing key is misused, or which deploys defective game logic may transmit correctly signed but incorrect data. Hub88 therefore applies consistency controls to the content of received data in addition to validating its origin.

Data consistency controls.

The following controls apply to data received from suppliers and to transactions processed by the platform:

- **Duplicate and replay detection** - Transactions are checked for repeated or replayed identifiers, so that a previously processed transaction cannot be submitted or settled a second time.
- **Payout and return-to-player deviation monitoring** - Realised payout behaviour is monitored against expected return-to-player values, and deviation alerting is in place. Detection of wins exceeding the maximum defined for a game is also in place, with a defined workflow governing the action to be taken upon such an alert.
- **Reconciliation** - Transaction totals are reconciled per supplier monthly, as part of the invoicing process. A mismatch is investigated and, depending on the outcome of that investigation, may result in manual reconciliation.

Feed monitoring.

Supplier latency and throughput are monitored at cluster level, and abnormal transaction volume or latency triggers an alert for investigation.

Suspension and resumption.

Hub88 maintains the technical capability to disable an individual supplier integration or game title without a platform release. Where the integrity of supplied content or data cannot be assured — whether by reason of a detected anomaly, notification from the supplier, notification from the CGA, or a lapse in the supplier's required certifications — the affected content is disabled until integrity is re-established. Affected operators are notified, and where the circumstances meet the notification criteria in Section 9 of this policy, the CGA is notified accordingly.

Supplier inventory.

Hub88 maintains a record of the suppliers, game content aggregators, and platform providers with which it integrates. For each, the record identifies the nature and scope of data exchanged, the internal owner, the contractual security and integrity obligations, and the certification or audit status of the provider. The record is reviewed at least annually and upon any change of provider or service.

Third parties, whether suppliers or partners, are subject to a Third-Party Risk Assessment undertaken at the onset of the relationship, recorded, risk rated, and regularly reviewed. Due diligence is required prior to the signing of any agreement for any gaming vendor or supplier whose software is customer-facing, and for any engagement where sensitive customer or company information is disclosed. The due diligence record captures corporate identity, ownership, ultimate beneficial owners, source of funds, and gaming authorisations held. Directors, shareholders, and beneficial owners are screened against politically exposed persons and sanctions databases using third-party screening providers. The Legal and Compliance Department owns this process.

Allocation of responsibility.

The Legal and Compliance functions manage contractual arrangements with third parties, together with the anti-money laundering and know-your-customer due diligence applied to them, as described above. That due diligence addresses legal and corporate requirements and does not assess information security risk.

The information security function maintains the third-party security risk assessment policy and holds the supporting security risk register. The register records, for each vendor, the classification of data exchanged, the internal technical owner, the contractual security obligations applicable to the engagement, the outcome of the assessment together with the evidence relied upon, and the date of next review. Assessments are performed during onboarding, upon material change to an engagement, and periodically thereafter, with the depth of assessment proportionate to the risk presented by the third party.

Contractual assurances.

Agreements with suppliers and content aggregators include requirements for security controls, notification of security incidents affecting supplied content or data, data integrity guarantees, maintenance of required certifications with prompt notification of any lapse or change in scope, and the right to audit or to request evidence of compliance.

Suppliers are selected on merit and Hub88 deals only with suppliers who comply with applicable legal requirements. Confidential information received from a supplier is treated as though it were Hub88's own confidential information. Agents, consultants, contractors, and representatives who have access to confidential information are provided with the Code of Business Conduct, are required to acknowledge it and are bound by its terms, and are retained only pursuant to a written contract approved by the Compliance Officer. Disclosure of confidential information outside Hub88 occurs only after appropriate confidentiality agreements are executed, copies of which are provided to the Compliance Officer.

Supplier agreements contain express provisions covering information security controls, notification of security incidents, data integrity, and the right to audit. This has been confirmed by the Legal function.

Gaming authorisations held by a supplier, including the issuing authority, licence number, issue and expiry dates, and current status, are captured through the due diligence process, and suppliers confirm that their gaming authorisation has not been revoked or suspended. Third parties are re-reviewed on a cycle determined by risk rating, at intervals of thirty-six months for low risk, twenty-

four months for medium risk, twelve months for high risk, and six months where a politically exposed person is involved.

Ongoing Monitoring.

The re-review cycle applied under the third-party risk assessment is calibrated to money laundering and terrorist financing risk and is proportionate for that purpose. It is not a measure of gaming certification currency, and its intervals for lower-risk third parties exceed the period permitted for certification verification. Hub88 therefore operates a separate certification verification cycle, independent of and in addition to the third-party risk assessment re-review cycle.

The certification status of every supplier whose game content is in active distribution is verified at intervals of no more than twelve months. Verification records the issuing authority, the certificate or licence reference, the scope of certification, the issue and expiry dates, and the current status, and is retained as evidence.

Expiry tracking.

Annual verification establishes a minimum. Because a certification may lapse at any point between scheduled checks, the recorded expiry date of each certification is tracked and reviewed in advance of expiry, so that renewal is confirmed before the certification ceases to be valid rather than discovered at the next annual cycle. Verification is additionally performed on the occurrence of any of the following: notification by the supplier of a lapse, withdrawal, or change in the scope of its certification; notification by the Curaçao Gaming Authority concerning a supplier's certification status; the introduction of new game content from an existing supplier; and any material change to a certified component.

Consequence of lapse.

Where a required certification is found to have lapsed, been withdrawn, or been narrowed in scope such that content in distribution is no longer covered, the affected content is disabled in accordance with the suspension procedure described above, the affected operators are notified, and the Curaçao Gaming Authority is notified. Distribution resumes only once valid certification is confirmed and recorded.

Supplier agreements require the supplier to maintain the certifications applicable to the content it supplies and to notify Hub88 promptly of any lapse, withdrawal, or change in scope. This forms part of the contractual assurances described above.

The Compliance function maintains a register recording the certification status of each supplier and reviews it annually.

11.6 Logging and Monitoring

Hub88 generates, retains, and monitors records of system and user activity sufficient to support the detection of security incidents, the attribution of actions to individuals, and the reconstruction of events for regulatory and forensic purposes.

Attribution.

A unique identifier is assigned to each person with access to the environment, so that actions taken on critical data and systems can be traced to a known and authorised user. Users are required to be identified by a unique user ID before being granted access to system components, and shared credentials are prohibited.

Monitoring and alerting.

Servers and network devices are continuously monitored, with alerts raised upon detection of unusual occurrences. The monitoring system produces reports covering server resource usage, changes made to networks and servers, and capacity planning. Devices and servers are configured to track access by employees.

Log retention.

Syslog data is stored at an offsite backup location and retained for a minimum of six years. Where local law requires a longer period, the applicable requirement for each jurisdiction is defined in the Hub88 Group Data Retention Policy. Access to stored backup and log data is restricted to Root-level personnel as defined under the access classification scheme.

In accordance with the applicable baseline, logging covers gameplay and betting transactions, high-value events, administrative access, and changes to system configuration.

Logs are forwarded to a centralised, tamper-resistant store. Log integrity is protected through cryptographic hashing or write-once storage. A documented periodic review of logs for anomalies is performed, and logging requirements are documented by system type. Management-plane activity, network flow, and administrative access events are recorded and retained, and threat detection is applied to that telemetry through Amazon GuardDuty. Supporting evidence is maintained in the form of platform monitoring and audit dashboards.

It is noted that the section of the Hub88 Group Security Policies and Procedures titled "Logging Process" addresses user authentication and session locking rather than audit logging, and that audit logging provisions are located elsewhere in that document. This will be addressed at the next review of the Group policy.

11.7 Malware Defence and Removable Media

Hub88 maintains defences against malware across its endpoints and infrastructure and controls the use of removable media in order to limit both the introduction of malicious code and the unauthorised removal of data.

Endpoint protection.

Corporate anti-virus software is deployed as part of every desktop and laptop build, and all Windows computers are required to run active anti-virus and anti-malware software. Tampering with anti-virus or anti-malware software is prohibited, as is the creation or distribution of malware. Devices used for remote working must carry up-to-date virus protection and the latest security updates.

Email and web.

The corporate email system incorporates virus and malicious code scanning, blocking such content before delivery to the client. Users are instructed not to open attachments from unknown or suspicious sources, to verify with the sender where a known source appears suspicious, and to notify the incident management team where an unknown source appears suspicious. Web browser and removable media risks are addressed in the annual security awareness training.

Server protection.

Servers hosting the gaming environment are excluded from third-party files and software and run only proprietary applications, and updates deployed to production are subject to review and confirmation through controlled channels. On that basis these servers do not carry an anti-virus agent. Other application servers employ anti-virus software, with database files excluded from scanning so that the operation of the remote gaming systems is not affected. This constitutes a

documented exception to blanket anti-malware deployment, supported by the compensating controls described.

Removable media.

Autorun and autoplay are disabled on managed endpoints through device management configuration. For equipment holding information classified at Confidential, Restricted, or Internal and External levels, available ports and removable media are deactivated in order to prevent the removal of data, and security labels are applied to indicate tampering. Where the use of removable media is required, it is subject to prior authorisation, and data transferred from external storage is scanned before use.

11.8 Backup and Data Recovery

Hub88 maintains backup and recovery arrangements sufficient to restore critical data and systems following incident, failure, or corruption, and to meet its regulatory data retention obligations.

Backup arrangements.

Backup is provided through Amazon Web Services. Daily snapshots of database instances are taken and stored securely, and access to backups is restricted to Root-level personnel as defined under the access classification scheme. Transactions and other significant data older than three months are archived to an offsite backup location and retained for a minimum of six years, in accordance with the Hub88 Group Data Retention Policy, which sets out the applicable requirement for each jurisdiction.

Protection of backup data.

Data held on computer media is stored in encrypted form, and encryption keys are classified as Confidential with access limited to technical personnel requiring such access. The access controls applied to backup data are equivalent to those applied to the corresponding production data.

Recovery testing.

Restoration from backup is tested on a monthly basis, and recovery point and recovery time objectives are defined for platform components.

Offsite backup.

Archived data is held in an offsite backup arrangement, so that a copy of archived transactional records is retained independently of the primary cloud environment for the duration of the applicable retention period.

11.9 Business Continuity and Operational Resilience

Hub88 maintains business continuity and disaster recovery arrangements designed to preserve the availability and integrity of the aggregation platform during disruption, and to ensure that information security is maintained throughout.

Resilient architecture.

The platform is deployed across multiple availability zones, providing redundancy in the event of the loss of a single zone, with automated failover between zones. Cross-region recovery capability is maintained in a separate geographic region.

Recovery objectives and testing.

Recovery point and recovery time objectives are defined for platform components, and restoration from backup is tested monthly.

Escalation.

Disruption meeting defined severity criteria is escalated internally and, where the circumstances meet the notification criteria set out in Section 9 of this policy, reported to the Curaçao Gaming Authority within the required timeframe.

Information security requirements continue to apply during disruption and recovery. Changes made under emergency conditions remain subject to the change management process, recorded and reviewed after the event, as set out in Section 9 of this policy.

Fallback procedures are defined for platform components.

The continuity plan is exercised twice annually and is additionally reviewed following any significant change to the environment.

A single continuity and disaster recovery plan applies across all jurisdictions in which the group operates. A jurisdiction-specific plan is not required for Curaçao; the requirement is that the plan accurately describes the arrangements protecting the platform, and that obligations differing by jurisdiction are identified as such.

11.10 Asset Management

Hub88 maintains visibility over the infrastructure, software, and content assets supporting its gaming operations, so that unauthorised or unsupported assets can be identified and addressed.

Infrastructure inventory.

The production environment is defined and managed as infrastructure as code using Terraform. The Terraform configuration and state therefore constitute the authoritative inventory of the cloud resources supporting the platform, including compute, database, storage, load balancing, and network resources. Because the environment is provisioned from code, the inventory is complete by construction, version controlled, and reproducible on demand.

Resource ownership.

Access to cloud resources is scoped to the teams responsible for the services they support, so that the group accountable for a given resource is identifiable from the access model. The inventory is reviewed periodically to confirm that resources remain required and correctly attributed.

Detection of unauthorised resources.

Because the environment is managed as code, any resource created outside the Terraform configuration is identified as configuration drift when the declared state is evaluated against the live environment. Drift detection therefore provides the mechanism required by the applicable baseline for identifying assets appearing in the environment without authorisation. Where drift is identified, the resource is either brought under configuration management or removed.

Software inventory. Application dependencies are declared and version-pinned in the source repositories, and the contents of deployed container images, including operating system packages and bundled dependencies, are enumerated on every build by the image scanning process described in Section 11.2. Together these artefacts constitute the software inventory for the platform.

Game content inventory. The game titles distributed through the platform, together with the supplying provider and the version of each integration, are recorded within the platform. This record serves as the inventory of game software contemplated by the applicable baseline and is maintained in conjunction with the supplier inventory described in Section 11.5.

The record can be produced as a reportable inventory on request, recording title, provider, version, and integration date.

Support status of software.

Verification that software in use remains supported by its vendor is performed as part of the monthly vulnerability and base image review described in Section 11.2. Components approaching or past end of support are identified and either upgraded or recorded as documented exceptions with compensating controls, under the same risk acceptance process applied to vulnerabilities. The quarterly review covers end-of-support status for base images, operating system and runtime versions, and third-party dependencies, in addition to known vulnerabilities.

Resource classification.

Assets are additionally classified by category and access level, covering keys, source code, binaries and images, documentation, equipment, and databases, with defined handling and protection measures for each combination of resource and clearance level.

Corporate devices and network.

Any device not authorised by the IT department, including personal laptops and mobile devices, is not permitted on the corporate network without prior approval. Dedicated guest networks may be provided for visitors, and Hub88 reserves the right to monitor and scan its networks to confirm appropriate use. Devices used for remote working are supplied by Hub88, and remote working on other devices requires written permission.

Corporate end-user devices are managed through a mobile device management platform, through which password, lockout, and configuration policy is enforced. An information technology asset management system is additionally maintained, recording assets and their assigned owners. Documented procedures govern the addition and removal of assets, the acceptable use of assets, and the secure disposal or reuse of assets at end of life.

Physical hardware underlying the production environment is managed by the cloud provider under the shared responsibility model. Hub88 does not operate gaming terminals, slot machines, or other land-based gaming hardware; the corresponding provisions of the applicable baseline are therefore not applicable to its operating model.

11.11 Data Classification and Protection

Hub88 classifies information according to sensitivity and applies handling, access, retention, and disposal controls appropriate to each classification.

Classification scheme.

Information and resources are assigned one of four classifications, each with a corresponding security clearance level: Confidential (ROOT), Restricted Access (MASTER), Internal and External Access (ADVANCED), and Public Access (BASIC). Personnel are cleared to a level and contact with resources above that level is prohibited. Documented handling procedures define the access policy, and protection measures applicable to each resource type at each level.

Need-to-know.

Access to sensitive information is granted only where there is a business need together with the appropriate personnel security clearance. Casual access to protectively marked assets is not permitted, and all personnel are made aware of their responsibility in applying this principle.

Protection in storage and transit.

All data relating to Hub88 activities transmitted over any communication network, including wireless networks, is sent in encrypted form, and information stored on computer media is held in encrypted form. Gaming transactions and game play are carried out over secure communication protocols.

Retention and disposal.

Retention periods are defined by data category and jurisdiction in the Hub88 Group Data Retention Policy, with a default minimum retention of six years for archived transactional data. Secure disposal is performed in accordance with recognised media sanitisation standards.

The categories of data processed by the platform are limited. Hub88 does not collect personal data from players; player identity data is held by the operator, and the platform processes pseudonymous identifiers together with transaction and game event records.

Inventory of data locations.

A central inventory is maintained recording the locations at which sensitive data is stored, processed, and transmitted, covering managed databases, storage services, and backup repositories. Each entry is labelled by data type and classification. The inventory is reviewed at least annually and upon any significant change to the infrastructure.

Encryption of end-user devices.

Full-disk encryption is enforced on corporate laptops. macOS devices are managed through Jamf Pro, with FileVault 2 enabled as a mandatory step of the enrolment workflow such that a device cannot complete enrolment without it. Windows laptops are protected by BitLocker. Mobile devices are protected by operating system encryption, which is applied once a device passcode is set.

11.12 Secure Configuration

Hub88 applies secure configuration to the systems, devices, and network equipment supporting its gaming operations.

Session locking.

Users are required to lock their workstation whenever leaving their desk, and screen savers are configured to activate after a period of no longer than five minutes, requiring a password to deactivate. Where there has been no activity, the system suspends the session and blanks the screen, requiring re-entry of credentials. This is more stringent than the fifteen-minute maximum specified by the applicable baseline for general systems.

Access attempt limits.

Access attempts are limited to no more than three before the account is locked, and only the system administrator may reset a locked account.

Secure management protocols. Administrative and remote access is encrypted, using SSH and secure transfer mechanisms, and is restricted where possible to defined source addresses with login under unprivileged accounts. All traffic entering or leaving servers is encrypted by default unless specifically permitted to be unencrypted, such as content delivery.

Network device credentials.

All internal network devices, including routers and firewalls, are assigned unique passwords, so that the compromise of one device does not lead to the compromise of others. Passwords are never hardcoded into software developed or modified by Hub88.

Documented hardening guidance is maintained for the cloud environment, and session timeout configuration is applied to administrative access.

The hardening guidance is subject to annual review.

Insecure protocols.

File Transfer Protocol and Telnet are disabled across the environment. Unencrypted HTTP is used only for communication between internal services within the private network; no externally reachable service accepts unencrypted HTTP.

11.13 Access Control and Authentication

Access to Hub88 systems and data is granted through a controlled process, authenticated by multiple factors, and withdrawn promptly when no longer required. This section should be read together with Section 11.1, which addresses account lifecycle and privileged access.

Provisioning.

Every user passes through a registration process forming part of the new employee onboarding process in order to gain access to IT systems. Each user is issued dedicated credentials for their exclusive use, which must not be shared, and the individual is accountable for all actions taken under those credentials. Credentials are added or removed only on the explicit instruction of Human Resources or the Head of Technical Operations.

Multi-factor authentication.

Two-factor authentication is required on all company-linked accounts. Remote access is provided through VPN secured by private and public key cryptography, with VPN account creation approved by the CEO or the CTO or COO. This satisfies the requirement of the applicable baseline for multi-factor authentication on externally accessible applications, remote access, and administrative access to core systems.

Revocation.

All access is revoked immediately from terminated users. Where an account, credential, or password is compromised or suspected of being compromised, the user must raise an incident report and inform Technical Operations immediately, and every password on an affected system is changed where a system is suspected of compromise.

External parties.

External parties granted accounts or access are subject to the Hub88 external party security policy. Credentials are personal, passwords must be changed at first login where key-based authentication is not used and every six months thereafter, the scope of work for the access is defined, and Hub88 reserves the right to revoke access at any time.

Recertification of access.

Existing access is recertified quarterly. Reviews are carried out by the security function, confirming that each account remains required, is assigned to a current individual, and holds an appropriate level of privilege. Findings are actioned through the provisioning and revocation processes described above.

11.14 Web and Email Protection

Hub88 reduces exposure to malware and phishing delivered through web browsing and electronic mail.

Email.

The corporate email system incorporates virus and malicious code scanning, which blocks such content before it reaches the client. Procedures for the handling of suspicious messages and attachments, and for their escalation to the incident management team, are set out in Section 11.7 of this policy.

Browsing. Web browsers are recognised as a common entry point for malicious code. All Windows computers are required to run active anti-virus and anti-malware software, and user awareness of browser-related risk is addressed in the annual security awareness training.

Domain name filtering.

Filtering of name resolution to block access to known malicious domains is provided across all client machines through the Cloudflare agent deployed to managed endpoints. Browser and email client versions are not centrally enforced; endpoint protection and network-level filtering provide the corresponding coverage.

11.15 Network Infrastructure Security

Hub88 secures and maintains the network infrastructure supporting its gaming operations.

Network access.

Access to networks is protected by username and password, certificate, or equivalent authentication. Unprotected wireless networks are not permitted. Devices not authorised by the IT department may not connect without prior approval, and the individual connecting a device is responsible for its safety with respect to the network and other users. Hub88 reserves the right to monitor and scan its networks.

Perimeter and segmentation.

The internet firewall protects the network from unauthorised access, permitting only necessary access to internal servers through a policy-based rule set. Partners access the back office through a web browser only. Access to the environment is restricted to specific gateways over secure channels using VPN and SSH.

Remote access.

Remote access is approved by the IT department, is always encrypted, and is restricted as far as practicable, for example by permitting connection only from defined addresses and only under unprivileged accounts.

Network infrastructure is provided and managed by the cloud platform and by the content delivery and zero-trust provider. Firmware and software currency, including the retirement of end-of-life

components, is managed by those providers under the shared responsibility model and does not require separate action by Hub88

11.16 Physical and Environmental Security

Hub88 protects its premises, equipment, and information from unauthorised physical access, tampering, and environmental threat.

Hosting environment.

The production gaming platform is hosted on Amazon Web Services. Physical and environmental security of the data centres, including access control, surveillance, power, and environmental conditioning, is provided by the cloud provider under the shared responsibility model and is evidenced by the provider's independent certifications. Hub88 does not operate gaming floor equipment, terminals, or cash handling facilities; the land-based provisions of the applicable baseline are therefore not applicable to its operating model.

Office premises.

Entry cards are issued to and carried by all personnel and only authorised persons or those with business to transact are permitted to enter the office. The first person to enter and the last to leave are responsible for deactivating and activating the alarm system, and for confirming that windows and doors are closed at the end of the day. Personal items of value are to be locked away when brought onto the premises.

Equipment.

Equipment holding information classified at Confidential, Restricted, or Internal and External levels is kept in secure rooms, with ports and removable media deactivated, security labels applied to indicate tampering, portable equipment secured to the workstation by a locking device, and portable equipment stored in a locked room or safe when not in use. Databases are stored on encrypted hardware in a secure room.

Clear screen.

Users lock their workstation when leaving their desk and shut down or hibernate when leaving the office, subject to defined exceptions for machines hosting shared services.

Clear desk and clear screen.

Users lock their workstation when leaving their desk and shut down or hibernate when leaving the office. Documents containing sensitive and confidential information are handled carefully during working hours and properly secured at the end of the business day.

Cloud provider assurance.

Evidence of the cloud provider's independent security certification is obtained and retained and is relied upon for those physical and environmental controls that fall to the provider under the shared responsibility model.

11.17 Human Resource Security

Hub88 manages information security responsibilities throughout the employment lifecycle in order to reduce personnel-related risk.

Onboarding.

New personnel pass through a registration process as part of onboarding, are issued unique credentials generated by Technical Operations, and are required to change the issued password at

first login. All employees receive the password policy and acknowledge that they have read it, together with the other policies and procedures.

During employment.

Personnel receive annual training addressing information security, anti-money laundering, and fraud, as further described in Section 11.3. Users are accountable for all activity performed under their credentials.

Termination.

All access is revoked immediately from terminated users. All written materials acquired during employment, in whatever form, remain the property of the company and must be returned on termination.

Disciplinary process.

Failure to comply with the security policies is treated as misconduct and breach of contract, evaluated according to severity, and may result in disciplinary action or termination. Where a criminal offence is considered to have been committed, further action may be taken to assist prosecution.

Pre-employment screening.

Controls are in place to satisfy Hub88 as to the integrity of all employees and contractors, and appropriate vetting is undertaken. Candidates are interviewed and their curriculum vitae analysed before any offer is made. Following an offer, all proposed employees are vetted, comprising confirmation of employment history and qualifications, the provision of identity documents, disclosure of any criminal convictions, and a recent police or criminal conduct certificate. Enhanced attention is given to officers, directors, and any staff member carrying elevated inherent risk by reason of their role. A criminal records check is undertaken for any appointment to a senior position, and for any existing employee promoted to a senior position, and confirmation of a satisfactory check is provided to the regulatory authority where approval is required for a key person position.

Where documentation cannot be provided for non-key staff, the Directors may waive the requirement on a justified case-by-case basis. Supporting documentation is retained on the Human Resources file, and a register of all staff members is maintained within Human Resources.

Confidentiality obligations.

Employees, officers, and directors are required to safeguard Hub88's confidential information, defined to include trade secrets, know-how, records, data, plans, strategies, processes, business opportunities, and information relating to customers and suppliers. Disclosure without appropriate authorisation is prohibited, and where there is doubt, information is to be treated as confidential. These obligations continue after an individual's service with Hub88 has ceased. Documents containing sensitive and confidential data are to be handled carefully during working hours and properly secured at the end of the business day.

Acknowledgement.

At the commencement of employment or other service, and from time to time thereafter, each employee, officer, and director completes an acknowledgement and disclosure statement attesting to compliance with the Code of Business Conduct. Acknowledgements are retained by Human Resources.

Reporting channel.

In addition to the incident reporting routes set out in Section 9 of this policy, a confidential reporting channel is available to employees and other representatives for reporting suspected

breaches of law, regulation, or the Code of Business Conduct, including anonymous reporting. Reports are received by a designated Confidential Designee independent of the financial reporting function, are logged, investigated, and reported in summary to the Board. Retaliation against a person making a report in good faith is prohibited and is itself a disciplinary matter.

11.18 Legal and Regulatory Compliance

Hub88 identifies and complies with the legal, regulatory, and contractual information security obligations applicable to its licensed activities.

Responsibility.

The Legal and Compliance function advises on the application of the security policies and on compliance obligations and may be contacted directly by any member of staff. Policies are reviewed at least annually and additionally where circumstances require, including upon a new licence application, updates to applicable law, and improvements to internal procedures.

Data protection.

Obligations relating to personal data, including lawful basis, data subject rights, breach notification, and retention, are addressed in the Hub88 Group Data Protection Policy and the Hub88 Group Data Retention Policy, the latter setting out retention requirements by jurisdiction. Where processing is likely to result in high risk, a data protection impact assessment is carried out.

Financial crime.

Obligations relating to anti-money laundering and the countering of the financing of terrorism are addressed in the Hub88 Group Anti-Money Laundering and Counter Financing of Terrorism Policy, and the assessment of money laundering risk arising from new technology is addressed in the Hub88 Group Technology Risk Assessment Policy and Procedure.

Regulatory reporting.

Reporting obligations to the Curaçao Gaming Authority, including the submission of incident reports within twenty-four hours, are set out in Section 9 of this policy.

The Legal and Compliance function maintains a record of the laws and regulations applicable to Hub88, held in a secure location. Any change affecting Hub88 triggers a review of its impact.

11.19 Cryptographic Controls and Key Management

Hub88 applies cryptographic protection to data in transit and at rest and manages cryptographic keys as a controlled asset. This section complements Section 11.4, which addresses the protection of data in non-production environments.

Approved algorithms and strengths.

Proven standard encryption methods are used, and proprietary encryption technologies are not permitted. All traffic entering or leaving servers is encrypted by default unless specifically permitted otherwise. The default technologies are SSL, TLS, and SSH. Private key length is no less than 2048 bits for SSL and TLS, no less than 2048 bits RSA for SSH, and no less than 2048 bits for VPN.

Key custody.

SSL and TLS keys and certificates are held on the servers providing the encrypted service, and their management is limited to IT management members holding root-level access. SSH private keys used for management are encrypted and password protected, and any server-to-server key

without password protection requires approval by the CTO. VPN authoritative certificates and keys are held on the VPN server endpoints with access limited to management members holding root-level access.

Key generation, transfer, and classification.

Keys are generated only by the highest level of management or by an individual cleared at the highest level, and access to key generators is restricted accordingly. Keys are double encrypted using asymmetric encryption by means of PGP and GPG, and are transferred only by secure means, being delivery in person, courier, secure file transfer for external parties, or PGP encrypted email internally. All encryption keys used for Hub88 information are classified as Confidential, with access limited to technical personnel requiring it.

Recoverability.

Where encryption is used, the sole readable version of information is not deleted until it has been demonstrated that the decryption process is able to re-establish a readable version.

Platform API traffic is additionally signed as described in Section 11.5.

A dedicated cryptographic policy is maintained, addressing the use of cryptographic controls for the protection of information and the management of encryption keys.

Key lifecycle.

Keys are generated by the highest level of management or by an individual cleared at that level, and are double encrypted using PGP and GPG for transfer. Keys are held in a managed secrets store with access restricted to authorised technical personnel. Use is governed by the minimum algorithm and key length standards set out above. Retirement is event-driven rather than calendar-based: an operator's registered public key is invalidated upon that operator leaving the platform, and keys are additionally replaced on suspected or confirmed compromise, on departure of personnel with key access, and on deprecation of an algorithm or key length.

Register of cryptographic controls.

A register is maintained recording the cryptographic controls in use and their purpose: digital signature of platform API requests using RSA-SHA256, applied in both directions and providing authenticity and integrity; transport layer security providing confidentiality of API traffic; encryption of data at rest in managed database and storage services; PGP and GPG for the protection of key material in transfer; a managed secrets store for key storage; and SSH and virtual private network encryption for administrative and remote access. Any approved exception to these standards is recorded in the register together with its compensating controls.

11.20 Security Governance and Compliance Assurance

Hub88 maintains governance arrangements to ensure that its information security programme remains effective, compliant, and subject to continuous improvement, and to demonstrate compliance to the Curaçao Gaming Authority.

Oversight.

Each responsible function reports on implementation to senior management, and the CEO supervises implementation of the Group security policies. This policy is approved by the approving official recorded in Section 1.

Policy review.

The Group security policies are reviewed at least annually, and additionally where circumstances require, including a new licence application, updates to applicable law, or improvements to internal procedures. This policy is reviewed quarterly, in accordance with Section 1.

Established corrective action mechanisms exist in adjacent domains. The Compliance Officer maintains registers of internal and external disclosures and of enquiries from competent authorities, monitors the performance of controls on an ongoing basis, takes immediate corrective action where a deficiency is identified, and reports at least annually to senior management on the control environment and the results of testing. The Confidential Designee maintains logs of reports made under the Whistleblowing Policy, recording how and when each was received, the nature and results of any investigation, and the resolution, with a summary reported to the Board quarterly.

The Compliance function maintains a register of corrective actions arising from information security review, audit, incident, or regulatory inspection, assisted by the security function. The register records the originating audit, incident, or inspection, the relevant dates, and the action points, and each action is monitored to closure.

11.21 Incident Response Timeframes, Escalation and Notification

The incident response procedure applied by Hub88 is set out in Sections 5 to 10 of this policy. This section records the roles, timeframes, escalation arrangements, and notification obligations required by the applicable baseline, and should be read together with those sections.

Roles.

Defined roles are maintained for the management of incidents. The Incident Manager takes control of an incident, performs the initial categorisation and priority assessment, appoints an Incident Owner from the Executive team, establishes remediation teams, and manages escalation. The Incident Coordinator, generally the Incident Manager, logs the incident, keeps stakeholders informed, liaises with any third party involved, ensures a closure report is submitted, and facilitates the post-mortem. The Incident Owner is the primary Executive stakeholder and is responsible for the final report. The Incident Team comprises the Incident Manager, the primary business stakeholder on the Executive team, and on-call personnel from DevOps and the product hubs. The final closure report, containing a completed root cause analysis, is approved by the Managing Director before an incident is considered closed.

On-call coverage.

A weekly on-call rotation of technical personnel is maintained from DevOps and each product hub, providing continuous availability of technical responders.

Response timeframes.

An operational service level agreement defines response expectations by priority for service incidents affecting the aggregation platform, its integrations, and dependent third-party services. That agreement is maintained by the operational teams and reviewed periodically.

Classification.

A single operational priority scheme is in active use, comprising Priority 0 through Priority 3. It is applied consistently through a mandatory incident priority field on the incident record, which permits only those values. The Hub88 Group Incident Management Policy does not operate as a classification scheme; it states expressly that its feature table is not intended to specify the classification or resolution time of each category and provides high-level guidance while delegating classification to operational judgement. Section 6.2 of this policy describes the security characteristics by which an incident affecting information security is assessed; the operational priority determines the applicable response timeframe.

Response timeframes.

Priority 0 incidents carry a response time of up to five minutes and are addressed on a continuous basis irrespective of the time of day. Priority 1 incidents carry a response time of five to ten minutes and are likewise addressed on a continuous basis. Priority 2 incidents carry a response time of fifteen to thirty minutes. Priority 3 incidents are addressed during business hours. Incidents affecting information security are treated as Priority 1 for the purpose of response timeframes.

Resolution timeframes.

Hub88 does not publish fixed resolution times by priority. The root cause, scope, and remediation path of an incident are not known at the point of detection, and a fixed resolution commitment could not be reliably met across the range of incidents that may occur. This is a deliberate position rather than an omission.

In place of fixed resolution times, time-bound accountability is achieved as follows:

- **Per-incident targets** - The Incident Manager, in consensus with the Incident Team, establishes target timeframes for the individual incident where appropriate to its nature and severity.
- **Functional escalation** - Where an incident cannot be contained or resolved by the current remediation team, it is passed to a team with a different or higher level of expertise.
- **Hierarchic escalation** - Escalation up the management chain occurs where an incident is of a serious nature, where containment or resolution may take an excessive amount of time, or where established target timeframes are not being met or have been missed.

Escalation on failure to meet a target therefore performs the function that a fixed resolution service level would otherwise serve, without committing Hub88 to an outcome that is not within its control at the point of detection.

Availability.

An availability target of 99.9 per cent is maintained, with corresponding permitted periods of unavailability defined on a daily, weekly, monthly, and annual basis.

Notification to the Curaçao Gaming Authority.

Hub88 notifies the Curaçao Gaming Authority without undue delay and in any event within twenty-four hours of any security incident that compromises gaming integrity, affects player funds or personal data, or may impact regulatory reporting, system availability, or game fairness. This obligation and the content of the report are set out in Section 9 of this policy. Failure to notify within that period constitutes a breach of licence conditions under the LOK.

Internal escalation.

Incidents are reported to the Compliance function immediately upon identification, so that the Compliance function is able to notify the Authority within the required period. Where the Hub88 Group Incident Management Policy refers to a seventy-two-hour period, that period relates to data protection breach notification and does not displace the twenty-four-hour period applicable to notification of the Authority.

Notification to data protection authorities.

Where an incident constitutes a personal data breach, notification to the competent supervisory authority is made within seventy-two hours in accordance with the Hub88 Group Data Protection Policy. This is a separate obligation from, and does not displace, the twenty-four-hour notification to the Curaçao Gaming Authority.

Reporting and records.

An incident log is maintained by the Incident Coordinator throughout. On resolution a closure report is provided by the Incident Owner to the Managing Director. Between occurrence and closure the responsible business owner reports regularly to Operations meetings. Incident logs and reports are retained for a minimum of six years, may be archived one year after closure, and are securely destroyed on expiry of the retention period.

Stakeholder updates.

Internal status updates are issued at intervals of no more than thirty minutes for Priority 0 to Priority 2 incidents. Affected operators are informed through support tickets, through dedicated messaging channels, or by direct notification.

Contact directory.

An incident contact directory is maintained. Internal contacts are provided and kept current by the security function, and external contacts, including the Authority, the financial intelligence unit, law enforcement, and insurers, are provided and kept current by the Compliance function.