
Casino Secret Information Security Policy

Version 2.0– September 2023

Signature: 
Ekaterini Ioannou
Director

Contents

Contents	2
Intellectual Property Rights.....	4
Trademarks	4
Acknowledgement	4
Symbols	4
Foreword	5
1 Introduction	6
1.1 Purpose	6
1.2 Scope	6
1.3 Document Structure.....	6
1.4 Information Security Document Set	7
1.5 Document Review and Update	7
1.6 Associated or Referred to Documents.....	7
1.7 Abbreviations	8
2 Information Security Overview	9
2.3 Standards	10
2.4 Risk Assessment	10
2.5 Training and Awareness	11
2.6 Security Organisation and Management	11
2.7 Security Incident Reporting and Management.....	11
3 Access Control	12
3.1 Summary	12
4 User and Gaming account Record data Protection	12
4.1 Storage of User and Gaming account Record data	12
4.3 Credit Cards.....	12
4.4 Magnetic Stripe / Chip Cardholder Data	12
4.5 Data Transmission across Networks	12
4.6 Encryption and Key Holders	13
4.7 Policy, Processes and Procedures	13
5 Network Security.....	13

5.1 Firewall	13
5.2 System Passwords	13
5.3 Remote Access	13
Vulnerability Management Program	14
6.1 Anti-virus Software	14
6.2.1 Patches	14
6.2.3 Maintenance	14
7 Network Monitoring and Testing	14
7.1 Access Tracking and Monitoring	14
7.2 Testing of Security Systems and Processes	15
Attachment 1: CS Management Group	16
1.1 Group Overview	16
1.2 Membership	16
1.3 Meetings	17
1.4 Reporting	17
1.5 Security / Information Security Responsibilities	17
1.5.1 Reporting	17
1.6 Risk Management	17
1.2 Incident Management Guidelines	18
1.2.2 Reporting	19
1.2.3 Management	20
1.2.5 Evidence	20
1.2.6 Processes	20
Version Control	23
Approval	23
Distribution	23

Intellectual Property Rights

This document contains valuable trade secrets and confidential information of Casino Secret and its suppliers, and shall not be disclosed to any person, organisation, or entity unless such disclosure is agreed in writing in advance by Casino Secret and is subject to the provisions of a written non-disclosure and proprietary rights agreement or intellectual property license agreement approved by Casino Secret. The distribution of this document does not grant any license in or rights, in whole or in part, to the content, the product(s), technology, or intellectual property described herein.

Trademarks

Casino Secret a trademark of Casino Secret.

Acknowledgement

The author wishes to acknowledge and thank the various developers and information providers for the use of their documents and their assistance to produce this document.

Symbols

The following symbols may be used in this document.



This symbol signifies **NOTE**. This is specific information relating to the subject matter.



This symbol signifies **INFORMATION**. This is general information relating to the subject matter.

Foreword

“We consider Information Security as a cornerstone of our business and treat extremely seriously the security of information given to us particularly payment card information.

As a company, it is all our jobs to follow the policy described in this document and the processes and procedures that follow from it. This also applies to all our vendors, suppliers, and contractors.

As new threats to security arise or new standards are required, policies may be updated. It is the intention that Casino Secret continues to provide a secure environment for information and have robust processes in place to administer information.

Security is everyone’s business”.

The management team of Casino Secret

1 Introduction

1.1 Purpose

The purpose of this document is to provide a high-level description of the Information Security policies adopted and implemented by Casino Secret for its sites, systems, staff, and suppliers.

This document also references other Casino Secret documentation that relates to this policy and forms part of the Information Security document set.

1.2 Scope

This document describes the company policy regarding threats considered in its risk analysis and refers out to detailed processes and procedures in support of this policy.

It describes at a high level how the company complies with all the requirements of the various standards concerning Information Security.

This document also describes the requirement for the auditing and reviewing functions necessary to ensure compliance with this policy.

1.3 Document Structure

This document is structured to give some general knowledge about Information Security

The document is divided into sections dealing with specific policy areas required by the ISO27001. Each section lists applicable company policies, process, and procedure documents applicable to the ISO27001 requirements although we are not ISO27001 certified however we follow best practice.

Other policies that are required for Information Security beyond the scope of protecting User and Gaming account Record data are included where applicable so that a total policy document dealing with all aspects of Casino Secret Information Security is available.

Some company documents relate to more than one Information Security requirement although Information Security is not their main aim, for example, the Staff Induction booklet. These documents further distribute the Information Security Policies and are listed in the associated document list.

The Information Security Incident Management and reporting procedures have been attached to this document, Attachment 2, as it is felt that in an emergency if anyone needed clarification of what to do, this would be the first document they would check.

1.4 Information Security Document Set

The Information Security document set is shown below. Many of these Information Security policies and procedures also form part of other Casino Secret policies and processes.

At the present time, some information may exist in two documents where there is a different audience or document purpose. However, as all the documents are reviewed and revised, this situation will be avoided where possible.

The Staff Handbook, for instance, contains Information Security Code of Conduct which is also contained in the Internal Security Policy. This illustrates that security policies are permeating through all the company activities.

As all the company documentation is reviewed and updated, duplication of information will be minimised.

1.5 Document Review and Update

This document will be reviewed from time to time and at least annually following from the Information Security policy it describes.

The review of this document will take place yearly. Version control is provided at the end of the document.

1.6 Associated or Referred to Documents.

The following table lists documents that are referred to, associated with this document or that provide background information.

Casino Secret Document Title	Date or Version
User Access Control Policy	Latest
IT Acceptable Use Policy	Latest
Information Security Code of Conduct	Latest

1.7 Abbreviations

The following table lists abbreviations used in this document.

Abbreviation	Meaning
DR	Disaster Recovery
IRM	Information Risk Management
IS	Information Security
PAN	Primary Account Number
PCI	Payment Cards Industry
PCI-DSS	Payment Card Industry Data Security Standard
CS	Casino Secret

2 Information Security Overview

2.1 What is Information Security?

Information is an asset that, like other business assets, is essential to Casino Secret business and consequently needs to be suitably protected. As a result of increasing interconnectivity of the business environment, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Information exists in many forms. It can be printed, written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes or means by which it is shared or stored; it should always be protected.

Information Security is the protection of information from a wide range of threats to ensure business continuity, minimise business risk and maximise return on investments and business opportunities.

Information Security is achieved at Casino Secret by the implementation of a set of controls, including:

- Policies, processes, procedures,
- Organisational structures,
- Software and hardware functions.

These controls have been established, implemented, monitored, and are improved where necessary, to ensure that the specific security and business objectives of the organisation are met. The Information Security policies form part of and fully integrate with the other Casino Secret business management processes.

2.2 Why is it needed?

Information Security policy is needed to.

- Assure the individual privacy of Casino Secret customers and staff members and, to protect Payment Card Holder data, ensure its proper use, storage, and disposal,
- Prevent damage to Casino Secret business operations due to unauthorised disclosures,
- Protect funds, supplies and materials from theft, fraud, misappropriation, or misuse,

- Provide the documented, justified selection of physical, technical, and administrative security controls, which are cost-effective, prudent, and operationally efficient,
- Protect property and rights of contractors, suppliers, and other organisations,
- Ensure the integrity and accuracy of all company information assets,
- Protect Casino Secret information processing operations from incidents of hardware, software or network failure resulting from human carelessness, intentional abuse, or accidental misuse of the system,
- Ensure the ability of all Casino Secret operations to survive business interruptions and to function adequately after recovery.

2.3 Standards

The company aligns in its business activities, as far as possible, with all relevant standards and codes including the two major relevant Information Security standards: PCI-DSS which is concerned with payment card data is managed by Payment IQ our outsource payment gateway and the broader ISO Standard 27001 that covers all Information Security areas.

Other company management policies and procedures conform, at a minimum, to their respective standards and codes of practice which integrate with our Information Security standards.

2.4 Risk Assessment

The protection of data and systems is never perfect. There is always some risk involved. Risk assessments have identified, quantified, and prioritised the risks against criteria for risk acceptance and objectives relevant to Casino Secret.

Risk assessments are performed periodically to address any change in the risk situation or the security requirements. The results of the risk assessment have and will determine management action and controls to protect against these risks.

The identified risks have been evaluated and reduced by implementing controls. The controls covered by this policy reduce the risks to an acceptable level for the business and to satisfy the Payment Card Industry Security Standards Council requirements.

2.5 Training and Awareness

Casino Secret requires its managers and team leaders to ensure that their staff are aware of the company Information Security policies and are fully aware of those policies and procedures that concern their activity in the company.

New staff induction procedures include the need for staff to understand the Information Security policy and how it relates to their job.

Suppliers and contractors are also made aware of the security aspects where they relate to their job or product. Clauses concerning Information Security are included in contracts and agreements with third parties where applicable.

From time to time and with a maximum period of 12 months between events, seminars are conducted, or other training is given to keep staff up to date with the policies and procedures.

2.6 Security Organisation and Management

At Casino Secret everyone employed and contracted is involved in security. It is part of their job or contract.

The Human Resources and IT department share a large part in implementing and monitoring our Information Security policies.

At a high level, the Board has much of the responsibility for:

- reviewing compliance and security risks,
- reviewing risk management procedures
- identifying significant risks
- monitoring effectiveness of procedures,

2.7 Security Incident Reporting and Management

Casino Secret has set up a dedicated email for all staff to report incidents itsupport@casinosecretgroup.com.

This ensures that Information Security events and weaknesses are communicated as quickly as possible allowing timely corrective action to be taken.

Processes and procedures are in place to deal effectively with security events or weaknesses once reported. The management team have the responsibility to apply a process of continual improvement to the reporting, evaluation, and overall management of these incidents.

Incident reports must be generated and communicated by director further if required by law. Where evidence is required, it is collected as quickly as possible and is collected ensuring compliance with legal requirements.

These processes are more fully described in Attachment 2 of this document.

3 Access Control

3.1 Summary

Casino Secret warrants to keep and maintain a dedicated Access Control Policy which is to prevent unauthorised physical access, damage and interference to the company's premises and information. Please reference this directly.

4 User and Gaming account Record data Protection

4.1 Storage of User and Gaming account Record data

User and Gaming account record data is known by Casino Secret staff and suppliers to be security sensitive and as such is not stored away from the secure servers where it was deposited. No copies are made or written down without director authority. This would only be given after risks were assessed. The data is particularly protected by the Casino Secret User Access Control policy.

4.3 Credit Cards

It is prohibited to store card numbers or validation codes, CVV2 numbers (three-digit value on signature panel), in the database.

4.4 Magnetic Stripe / Chip Cardholder Data

Full Magnetic Stripe / Chip Cardholder Data is not at this stage collected by Casino Secret., Card holder data is stored by Payment IQ who are Level 1 PCI Compliant.

4.5 Data Transmission across Networks

All data sent externally to/from Casino Secret facilities is encrypted.

SSL, TLS 1.3 is used on our websites where customers enter registration and User and Gaming account Record data.

IPSEC is used to encrypt data over public networks to our remote sites Our Payment Service Providers are PCI compliant.

4.6 Encryption and Key Holders

At present User and Gaming account Record data is held and managed in third party systems with appropriate security certification (ISO27001, PCI, SOC2 or SOC3).

4.7 Policy, Processes and Procedures

The following policy, process and procedure documents detail the implementation of the User Access Policy, except Network Security.

5 Network Security

5.1 Firewall

All access points where the Casino Secret network meets public networks are protected with hardware Firewall devices installed at each individual location.

Web servers are located outside the internal network and separated from it by firewalls.

5.2 System Passwords

All supplier default passwords are changed and installation guides for network devices are followed.

Production systems (servers and network components) are hardened by removing all unnecessary services and protocols installed by the default configuration.

5.3 Remote Access

All Remote Access computers connecting to the internal network are secured by an encrypted VPN (Virtual Private Network) and have their own personal firewalls and antivirus software. This is covered by the *Casino Secret Acceptable Use Policy document*.

All external suppliers and vendors are subject to the Remote Access rules. Any change in the security, processes and management of the third-party suppliers and vendors is monitored. Any change in IT policies is communicated to vendors to be observed immediately. The failure in the compliancy of the IT policies can result in the banning of the vendor or supplier. Security provisions are introduced in the service contracts between IT and every vendor with access to the system.

Vulnerability Management Program

6.1 Anti-virus Software

All potentially vulnerable machines used in Casino Secret have anti-virus protection software deployed with automatic updates activated. 6.2 Systems and Applications

6.2.1 Patches

The latest vendor supplied security patches are installed, after testing, on all system components and software.

The IT Department maintains a careful watch on newly discovered security vulnerabilities and installs automatically updates through MS Intune.

6.2.3 Maintenance

Implementation of software modifications and security patches follow the change control procedures and policies of our external software suppliers. We do not own our own code.

7 Network Monitoring and Testing

7.1 Access Tracking and Monitoring

Logging systems are to be deployed listing all access, including administration access.

System clocks are synchronised to provide accurate date and time stamping in logs. For our platform supplied by Optima the synchronization is made with the Atomic Clock maintained by the Instituto Nacional de la Armada Española (Spanish National Army institute).

Regular reviews of firewalls and routers are undertaken to monitor for unauthorised traffic.

7.2 Testing of Security Systems and Processes

Vulnerability scanning on all systems is performed before they are placed into the production environment by our platform providers.

Penetration testing is carried out periodically where appropriate by third party expertise by our platform providers.

For local IT environments we use Microsoft Intune which checks for vulnerabilities to local networks and machines using Microsoft Defender.

Attachment 1: CS Management Group

1.1 Group Overview

As a result of several requirements of the various standards, codes and acts that Casino Secret must comply with as part of its license conditions and as part of good business practice, the management group meet to handle matters such as:

- Information Security
- Legal and Regulatory Compliance
- Anti-Money Laundering
- Responsible Gambling / Self Exclusion
- Review compliance with the proposed industry codes of practice
- Accounting /Regulatory Returns
- Review and identification of Risks

This group will also ensure that any required documentation, reports, or returns are being made available when and where required.

From time to time, the various functions/membership of the group will be reviewed in the light of any new requirements that come up.

It is important to note that, on a day-to-day basis, CS staff are still responsible as required on matters such as Information Security within their normal reporting structure.

1.2 Membership

The group consists of several permanent members with areas of responsibility and expertise. These areas reflect most of the main requirements in the proposed Code of Practice where we need to show affirmative activity both in reporting record keeping and documentation.

Other areas may require reports or attendance by other Managers when appropriate.

Permanent Members:

- CTO
- COO
- Head of Finance
- Head of IT
- Head of Product

1.3 Meetings

The group will meet when required such as during an incident or if a vulnerability requiring mitigating action is discovered.

Minutes will be taken but will be of a short form i.e., Actions proposed or taken, Results of discussions rather than full details of proceedings.

The minutes and associated papers will be archived to provide auditable records.

1.4 Reporting

The minutes, any reports, actions, or recommendations resulting from the group meetings will be recorded.

1.5 Security / Information Security Responsibilities

1.5.1 Reporting

Reports of any security incidents will be available at the group meeting for assessment and checking that present procedures are adequate.

1.6 Risk Management

Part of the group's function is to review risk, risk management procedures and identify significant risks regarding Compliance and Security.

To achieve this goal, the group may require assistance, information, and analysis from any area in the company.

As the management group is most senior in the business any decisions made and actions to take will be considered as approved.

Attachment 2: IS Incident Management

1.1 Overview

This incident management procedure gives guidelines concerning the typical actions that should be taken by the various staff and groups within Casino Secret. Many types of incidents can happen and to a great extent an amount of common sense needs to be applied to the process as most incidents are unique.

Simply, the process is:

- A security incident or suspicion is reported to a Line Manager, HR, IT manager or senior manager and to itsupport@casinosecretgroup.com
- Corrective action is taken by the above people, if possible, to limit damage and exposure,
- The incident and action are reported to the Head of IT who may consult with others as to what further action needs to be taken,
- A report of the Incident is made available to the management team.
- The management team discusses the incident and action taken and may require new procedures to reduce the risk in the future.

The sections below detail the guidelines to be used for incident management.

1.2 Incident Management Guidelines

1.2.1 Data Classification.

Data types within the Casino Secret system can be classified in six groups:

- 1) Customer account information including personal, access and financial information,
- 2) User banking and payment details information.
- 3) Gaming transaction information.
- 4) Payment transaction information
- 5) Marketing campaign information.
- 6) Other information.

All data is considered critical regarding incident management.

All data is stored in the main DB instance and is treated at the same level in terms of maximum security, backup and recovery measures by Optima or our other supporting software vendors.

1.2.2 Reporting

It is the responsibility of all staff, contractors, and third-party users to report any Information Security incidents as quickly as possible.

Staff should report any suspected event to one of the following as appropriate:

- their line manager, in the first instance, the IT Manager, a company Director with the incident severity.
- itsupport@casinosecretgroup.com

Information Security incidents are classified into three levels by Casino Secret. These levels are described in the table below.

Level	Typical Incident Type
3	User rights infringed; company rules not followed. Internal User password compromised shared etc. Remote access agreement not followed. Virus attacks (thwarted by anti-virus)
2	Security keys compromised. Unauthorised user on the network Variety of computer network attacks Visitor process not followed
1	Data classified on groups 1,2,3 and 4 stolen. Customer and Gaming account Record data stolen or compromised. Company assets stolen resulting in business operations halting. Forced entry into building and/or secure locations. Disaster Recovery required for Business Continuity

The first evidence or report of an incident may not show the true severity of the incident. So, an incident level may be raised (or lowered) as more knowledge becomes available.



Level 1 Information Security incidents may involve or have implications for other organisations that may come under different authorities. In these cases, reporting and evidence collecting processes will need careful conduct. Obtain advice from the legal department as soon as possible.

1.2.3 Management

1.2.3.1 Incident Coordinator

For extremely serious Level 1 incidents, an incident coordinator is appointed by the COO to be the central point of contact and for leading a response team.

For lower-level events the coordinator would automatically be the appropriate person from one of the following:

- the IT Manager
- the Head of Product

The coordinator will log all activities concerning the incident including times, staff, and witnesses.

1.2.3.2 Response team

A response team is formed by the coordinator in conjunction with the COO to deal with managing the corrective action, monitoring the situation, and collecting the required evidence.

1.2.5 Evidence

It is not always obvious at the outset of an incident exactly how serious it is and whether the event could result in court action. It is therefore important that the incident coordinator should decide as to what evidence to collect as soon as possible, erring on the side that more is better.

1.2.5.1 Physical

Keep the original securely with a record of who found it, where found, when found and any witnesses. The original should not be tampered with.

1.2.5.2 Electronic

For retention of information on computer media, mirror images or copies of any removable media, information on hard disks or in memory should be taken to ensure availability. Log all actions during the copying process and have a witness. Original should be held securely if possible. Any logs of network activity for the relevant times should be copied and kept. These activities should be witnessed.

1.2.6 Processes

1.2.6.1 Introduction

Two processes are used to deal with security events: the standard process for level 2 and level 3 events and the emergency process for the highest severity level 1.

The standard process for level 2 is a reduced version of the emergency procedure but the outcome will not result in court processes or involve external organisations. However, as disciplinary action may be taken by the company against the perpetrator if within the company and identified, suitable evidence should be collected.

Level 2 implies that:

- A coordinator can take required actions without reference to the management team.
- There is time to correct the situation,
- Further damage from the event is unlikely.

Level 3 events are dealt with at line manager level.

Such events as virus attack are dealt with by suitable anti-virus and are logged and reports are available for the management team. Level 3 events such as incorrect computer use, poor entry badge use would be reported to the staff member's line manager.

1.2.6.2 Information Security Emergency Response Process

An Emergency* Response is initiated by:

- escalation of a security event
- declaration by one of the management team of a security event

**Aside from information security events the business also has a guide on what to do for other emergencies and emergencies out of hours (duty manager) which is considered separate from an information security event.*

If an emergency response addressing information security is started, the most senior security staff member available at the time of the incident becomes by default the incident coordinator.

The coordinator assembles an incident response team which will include at the least representative from the IT Department.

Minutes are kept of the status, actions, and resolutions. The coordinator reports on the cost, exposure, and continuing business risk of the incident.

Next courses of action:

Lock-down and repair

Perform the actions necessary to prevent further damage to the organisation, repair impacted systems and perform changes to prevent a re-occurrence.

Reduction of level

Team decides this event did not warrant emergency response. Event handled as level 2 or 1 or even closed.

Monitor and capture.

If required, the team can perform a thorough investigation with continued monitoring to detect and capture a perpetrator. The COO must be involved.

Review and analyse log data, use forensic tools to determine nature and scope of incident.

There is the possibility of communication with various Law enforcement agencies or other outside entities. This should be handled by a director or the legal department.

Test and validate the repair.

The coordinator must be satisfied that the security breach has been properly repaired.

Complete report.

The management review event report and initiate any modifications to processes, procedures, tools, or applications felt necessary.

An important part of the management process is the management review of procedures and corrections from lessons learnt analysis.

Version Control

Version	Author	Comment	Date
1.0	CGB	Initial version	2018
1.0	n/a	No change	2019
1.0	n/a	No change	2020
1.0	n/a	No change	2021
1.0	n/a	No change	2022
2.0	JHR	2 nd Version – aligning to company structure and practice	29-09-2023

Approval

	Name	Date
Author	Nikos Petrakos	29-09-2023
Owner	Jeremy Harding Roberts	20-10-2023

Distribution

Department	Position
All internal departments	All staff
Casino Secret Ltd	All Management Team