



Information Security Policy

For the offering of Online Gambling Under Licence From CGB

POL-CU-IS-01

Current Version

Version	V1.0
Version Date	14-05-25
Contributors	Kalle Uusitalo - BetComply , Stephen - Grayspace
Approved by	NOT APPROVED (DRAFT)

Table of Contents

1. Overview	3
1.1 Introduction	3
1.2 Legal Scope	4
1.3 Definitions and abbreviations	4
2. The Policy	6
2.1 Types of Data	6
2.2 Acceptable Use and Ethics	7
2.3 Passwords, Access Control and Logging	8
2.4 Device Policy	8
2.5 Email Policy	9
2.6 Network Security	9
2.7 Wireless Communication	10
2.8 System Security	11
2.9 Firewalls	11
2.10 Malware	11
2.11 Intrusion Detection	11
2.12 Supplier and Third Party Relationships	12
2.13 Backups	12
2.14 Intellectual Property Rights	13
2.15 Retaining and Protecting Records	13
3. Recording-keeping	13

1. Overview

1.1 Introduction

Bull Gaming NV (“The Company/ Rollbit/ us/ our/ we”) has developed and put into effect this Information Security Policy (hereinafter referred to as the InfoSec Policy) to mitigate the integrity risks associated with providing licensed online gambling services in Curacao.

We seek to offer the highest security to all of our users and customers on Rollbit.com. For that, we will take all the necessary steps to ensure that our information security is of the highest possible level regardless of which format the data in question is in; electronic, written or printed on paper, stored electronically or on paper or spoken in conversation and minimising any possibilities of it being accessed, altered or destroyed. This means protecting it from internal and external threats, whether accidental or deliberate so that the business continuity is always maintained and any possible damage minimised.

Rollbit.com is committed to high standards of information security, according to EU and other international guidelines, compliance, and requires management and employees to enforce these standards in preventing the use of its services for money laundering purposes.

In accordance with the information security legislation, the board of directors of Bull Gaming N.V. is responsible for the information security and all things related to it on Rollbit.com. The InfoSec Policy has received approval from the Company's directors and is aligned with the broader compliance framework governed by the applicable laws and regulations for providing licensed online gambling services in Curacao. Each major change of Rollbit.com InfoSec policy is subject to approval by the managing director of Bull Gaming N.V.

1.2 Legal Scope

The primary legislation regulating the online gambling industry in Curacao is the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen). Additional laws and regulations on which this Policy is based consist of:

Laws and regulations	Abbreviation
the National Ordinance Identification for Services (Landsverordening identificatie bij dienstverlening, PB 2017, no. 92, GT);	NOIS
the Sanctions National Ordinance (Sanctielandsverordening, PB 2014, no. 55, GT);	SNO
the Kingdom Sanction Law	KSL

Unless specified, this Policy refers to the above legislation as "applicable laws and regulations".

1.3 Definitions and abbreviations

"Gambling interface" the whole of electronic communication with which we offer the licensed games of chance;

"Games of chance by means of distance communication": a game of chance that is organised remotely on the basis of the license;

"Hyperlink" includes an active icon;

"Licensee": the holder of a license granted pursuant to the NOOGH;

"Online Gambling" means any gaming, where any player enters or may enter the game, or takes or may take any step in the game, by means of a telecommunication, the negotiating or receiving of any bet by means of a telecommunication, or any lottery in which any participant acquires or may acquire a chance by means of a telecommunication

"Player": the person who is registered as a player with the licensee;

"Player account": the account held by the licensee in the name of a player with the playing balance of that player, which is used exclusively for the purpose of participating in the licensed games of chance and which can be traced back to the player;

"player interface": the part of the gambling interface accessible to the player after registration;

"**Website**", means an electronic communication or set of electronic communications which complies with the Hypertext Transfer Protocol and may be accessed and viewed in visible and legible form by any person having ordinary access to the global system of intercommunicating computers known as the Internet.

Definition	Abbreviation
Anti-Money Laundering	AML
Business Risk Assessment	BRA
Customer Due Diligence	CDD
Counter Funding of Terrorism	CFT
Customer Risk Assessment	CRA
Enhanced Due Diligence	EDD
Financing of Proliferation	FP
Curaçao Gaming Control Board	GCB
Know Your Customer	KYC
Money Laundering	ML
Politically Exposed Person	PEP
Source of Funds	SOF
Source of Wealth	SOW
Terrorism Financing	TF

2. The Policy

2.1 Types of Data

It is paramount to protect all different types of data at the level appropriate for them. The classifications are reviewed regularly and if necessary, re-classifying them as per their importance and/or sensitivity.

The different types of data are defined as:

1. **Public data** - This is data available to the public and can be considered as “non-classified”. It may however be subjected to rules or regulations as per the prevailing legislation and therefore needs to be handled in a certain way.
2. **Protected/internal data** = This data is largely not publicly available and includes material such as company documents and other sensitive information which could cause harm or significant negative impact on the company should it be made public. If this data would be disclosed publicly, it could cause:
 - a. *Harm/distress to individuals*
 - b. *Compromise third parties*
 - c. *Financial loss and/or facilitate improper gains*
 - d. *Individuals or companies to have unfair advantage*
 - e. *Breach legislation regarding disclosure of information*
 - f. *Investigations to be compromised*
 - g. *The company to be in an a disadvantageous position commercially*
3. **Restricted data** - This level of information could lead to even more serious consequences and possibly legal action against [Rollbit.com](https://rollbit.com). Information such as personal details, sensitive business processes, credit/transaction information etc. If this data would be disclosed publicly, it could cause:
 - a. *A negative impact on relationships with other organisations*
 - b. *Substantial distress on individuals*
 - c. *Significant financial loss and/or facilitate improper gains*
 - d. *Individuals or companies to have a significant unfair advantage*
 - e. *Investigations to be compromised or crimes to be facilitated*
 - f. *Severe breach legislation regarding disclosure of information*
 - g. *The company to be in an a disadvantageous position commercially*

This type of data is not handled commonly by individuals who aren't at least in a managerial position of some level, with access to lower level employees given only under special circumstances. This data is encrypted during transmission.

4. Confidential data - The highest level of security is reserved for the confidential data as this could have a major negative impact in all facets of the organisation if made public. Information such as development work, financial results or other production information which is crucial to maintain secret. Alongside the above, disclosing this data could cause:

- a. Material damages with other organisations*
- b. Risk to individual security*
- c. Operational effectiveness and security to be jeopardised*
- d. Facilitate serious crime and/or jeopardise investigation of such*
- e. Disruption of seizing of business operations*

Who has access to this data is very strictly controlled and generally only reserved for senior management who control access to it. This data is always encrypted.

2.2 Acceptable Use and Ethics

All devices which employees use are to be used in accordance with the [Rollbit.com](https://rollbit.com)'s policies and the use of such devices may be monitored.

The use of the company devices for personal profit is strictly prohibited and it is possible that the company limits the use of the devices for anything but work related activities.

Any software used on the company's devices must have the appropriate licensing.

Company devices absolutely cannot be used for illicit activities or facilitating illicit activities of any nature.

It is not permitted to perform vulnerability scans, monitor network traffic, or perform any action which would provide the employee information about the device, network or the systems which they should not see.

Users shall not reveal any information about the clients, employees, business practices, technology, schedules, or any other information regarding [Rollbit.com](https://rollbit.com) which is not already publicly available to any outside resource or person without expressed permission from the Chief Operating Officer.

2.3 Passwords, Access Control and Logging

To achieve proper information security, the first step is often ensuring that everyone in the organisation has proper passwords that are stored correctly and only the individuals who need access to certain data have access to it.

The most important points to achieving these are:

- Each employee is assigned a unique login which only they know
- Each device is password locked and the screen locks automatically after 5 minutes of inactivity
- Back-end systems have an automatic log-off after 15 minutes of inactivity
- All stored passwords must be encrypted
- Accounts that do not require MFA must have their password reset every 90 days
- Logged events
 - Date and time of all successful and unsuccessful login attempts
 - Date and time of access attempts to any data not classed as “public”
 - Date and time of changes to system, configuration or otherwise
 - All control system events
- Any personal information will be logged for a minimum of 5 years
- Account will be locked after multiple failed login attempts
- Accounts can be reset only by the system administrator
- Sharing of login details is strictly prohibited. Any exceptions to access to accounts is subject to approval by the Chief Operating Officer
- Access to third party systems (Game or payment providers for example) are strictly personal
- Any shared accounts must be subject to IP whitelisting
- All player data (login details, segmentation etc.) must be encrypted
- Dormant accounts are deleted after 12 months of inactivity

2.4 Device Policy

All devices (laptops, computers, phones etc.) that are issued by [Rollbit.com](https://rollbit.com) are considered to be the property of the company and need to be treated as such.

It is prohibited to use personal devices to conduct any type of [Rollbit.com](https://rollbit.com) business or access any of the systems and/or data.

Laptops are never to be left unattended or on desks overnight in the office. When in transit, laptops should be held in a laptop bag, out of sight and never checked in during flights.

If a laptop is lost or stolen, this needs to be reported without delay to the Chief Operating Officer.

All laptops and other devices need to be returned at the end of the employment. Any exceptions to this are subject to the approval of the Chief Operating Officer.

All laptops and other devices are recycled accordingly should they become obsolete at any point of the employment or after it has ended.

2.5 Email Policy

It is important to note that all messages that travel through the [Rollbit.com](https://rollbit.com)'s email system are the property of the company and they ultimately have access to all of these messages if necessary.

All employees are required to adhere to the following guidelines when using the company's email system:

- All attachments must be scanned for viruses and great care is exercised with unexpected attachments
- All sensitive data sent over email, whether text or attachments, must be encrypted
- Any virus warnings must be reported accordingly
- No copyrighted or sensitive material is to be sent via email, this is to be shared via Drive
- Emails must not contain offensive or any materials considered as harassment
- Employees are not to use their [Rollbit.com](https://rollbit.com) emails for personal or any other but business related use
- Any phishing or other scam emails must be reported and also reported via the email client's function as such

2.6 Network Security

Maintaining the necessary level of security throughout the network infrastructure is dictated by the requirements set by the following factors:

- The classification of the data being transmitted and access through the network
- Risk assessment of the network infrastructure
- Level of trust between the connected parties
- Business continuity level required
- Geographical location and spread of the network
- Security capabilities of the connected devices
- Security controls at the physical locations where network is accessed

All of the above shall be assessed and documented accordingly before the network is established.

In all cases, the network infrastructure design needs to also meet the following criteria:

- Defence in Depth mentality and Zero Trust Network Access
- Network and data flow diagrams shall always be updated as per PCI-DSS
- No connection to the internet until it is determined that all different classifications of data can be protected accordingly
- Segregation of network when processing payment card information of any sort
- Secure and encrypted communication only during remote administration

All network security must also be designed to meet the requirements of the risk assessment and the data being handled in proportion to both.

When using remote access, the following controls must be implemented:

- Secure VPN connection using SSL/TLS
- 2-Factor Authentication
- Access for clients who do not meet minimum requirements shall be restricted

All critical devices that are connected to the network must have an intrusion detection installed.

A detailed network diagram of the whole infrastructure is to be maintained and reviewed after each change to the network and these changes are to be reviewed and confirmed by the Chief Technical Officer.

An annual scan is performed to ensure that the diagram is correct and any devices that are not found in the diagram must be reported and investigated accordingly.

2.7 Wireless Communication

All wireless access points must be secured with a password or another method which prevents unauthorised access to the access points. These are to be configured to use WPA2 wherever possible.

The wireless network must be separated from the network which handles sensitive data by a firewall. The physical devices for access points must be hidden from view and not accessible easily.

Analysis of the wireless network is run regularly to detect any unauthorised devices connected to the network.

Bluetooth and Wifi must be turned off on all relevant devices when traveling to avoid connection to unsecured networks.

2.8 System Security

All systems which are connected to the internet must have the latest version of the operating system as well as the latest security patches installed on them and are subject to regular checks of the system integrity.

All player activity is always communicated over a secure communication channel and where possible, encrypted.

2.9 Firewalls

All firewalls must be set to “Deny” all traffic that is not explicitly allowed by the system administrators.

Like wireless networks, the firewall must also be scanned regularly for any unauthorized access to the network. Any changes made to accesses or the configuration of the firewall must be logged accordingly.

The configuration of the firewall needs to be set as per PCI-DSS and reviewed every 6 months. These configurations must be documented including the devices, protocols and ports with the business justifications.

2.10 Malware

It is absolutely forbidden to introduce malware or any other malicious software to the systems of [Rollbit.com](https://rollbit.com). Each employee, system and device used to connect to the internal systems must have a licensed antivirus and malware -software installed.

This also includes emails, which must be done by the software if the email client does not provide this service themselves.

Employees are not allowed to disable or tamper with their antivirus software and all scans must be logged accordingly. If the spread of malware is detected, the employee must do their utmost to contain the malware to their device and disconnect it from the network.

All company provided devices, workstations and servers must be installed up to a high security standard such as PCI-DSS and with up-to-date virus definitions.

2.11 Intrusion Detection

The Chief Operating Officer of Rollbit.com is responsible for ensuring that any possibilities of an intrusion are minimised through detecting weaknesses and performing appropriate testing.

Should a breach happen, it needs to be detected as soon as possible. In case of an intrusion, it is also their responsibility to ensure that data is not compromised and its integrity is maintained, the systems are not used for malicious purposes and that there is minimal disruption to the operation of the company.

It is also the responsibility of all employees to report any breaches or suspicions of a breach to the Chief Operating Officer who then investigates the case.

All intrusions or intrusion attempts must be logged and kept a minimum of 90 days.

2.12 Supplier and Third Party Relationships

All suppliers and other third parties who work with [Rollbit.com](https://rollbit.com) are required to adhere to the same security requirements as the employees of the company. This will be confirmed contractually and include an NDA.

The level of access given and the information shared with them depends on the tasks which they are carrying and only will be relevant to those tasks.

Should they need a remote connection to the systems and/or servers of [Rollbit.com](https://rollbit.com), this will only be done at the discretion of the Chief Operating Officer.

The appropriate due diligence is carried out to ensure that any third parties who we enter a business relationship with are legitimate businesses and operate in a legitimate way.

[Rollbit.com](https://rollbit.com) also ensures that the suppliers and their compliance with the regulations and our own policies is monitored throughout the relationship.

2.13 Backups

It is paramount for any business to back their data up in case disaster recovery, another catastrophic system failure or possibly a human or technical error which would cause significant disruption to the business operations and possibly.

[Rollbit.com](https://rollbit.com) backs their data up periodically via their remote servers. Restoration tests are carried out periodically, but at least every 6 months and the process is documented in the relevant documentation where the data is stored.

How long the backups are stored depends on the type of the data, as different data has different storage requirements. This means that each type of data is labelled accordingly and deleted when this timeframe has passed.

Each backup is handled with the same classification as the data contained in it. If the data needs to be disposed of or repurposed, the industry standard for treating such data will be applied.

2.14 Intellectual Property Rights

Any artefact or data created by an employee while employed by or under contract with [Rollbit.com](https://rollbit.com) is owned by the Company unless otherwise arranged through a written agreement between the two parties.

Should anyone want to use an artefact or any data owned by [Rollbit.com](https://rollbit.com) needs to request this in writing and state the intended use of the artefact. This request may or may not be accepted by [Rollbit.com](https://rollbit.com) at their discretion.

[Rollbit.com](https://rollbit.com) owns all the data and artefacts created by any third parties for the Company unless otherwise agreed in writing.

2.15 Retaining and Protecting Records

All records are held as required by all applicable legal, regulatory, and contractual requirements and only for the time during which they are required to be held.

Records shall be treated as per their classification and access to the records is determined accordingly. However, these are always available for business needs and regulatory authorities for auditing purposes.

3. Recording-keeping

The Company will maintain comprehensive records related to information security, breaches of this security, and any other relevant documentation.

Records will be retained for a minimum period of 5 years after the business relationship is ended or after the transaction date.

The records will be easily accessible to authorised personnel and relevant regulatory authorities for inspection or audit purposes.