

Information Security Policy

VERSION HISTORY

Version Number	Version Date	Author	Summary of Changes
V1.0			Initial Draft

APPROVALS

Name	Title	Date of Approval	Version Number

DISTRIBUTION

Name	Title	Date of Issue	Version Number

Contents

Background	4
Objectives.....	4
Access Control Policy	4
User Management	5
Information	5
Physical Access.....	6
Training And Responsibilities	7
Joiners, Movers, Leavers	7
Third Party Service Providers	7
VPN Remote Access	8
Password Management.....	8
Equipment, Devices, Media	8
Personal Devices	9
Network Security.....	9
Network Security.....	9
DMZ.....	10
Remote Access / Management	10
User groups	10
Application Protection	10
Security Awareness	10

Background

We are committed to safeguarding information of Joyeux B.V. (the “Company”) as an asset, not only to ensure that regulatory and contractual obligations are complied with, but also because we believe that having a streamlined procedure regulating access, use, disclosure and destruction of information in whatever form, and applying it across the board, ensures that all employees feel responsible for the information they are entrusted with which serves to reduce security incidents to a minimum, as well as financial losses, judicial proceedings and bans on data processing which often arise as a consequence of security incidents.

Objectives

The primary objective of this policy is to provide a security framework that will ensure that information is protected from unauthorised access, loss, or damage, and that will regulate the use, disclosure and destruction of information, whether or not belonging to the company, and whether physical or electronic, whilst in conformity with the principles of integrity, confidentiality and availability of information.

Access Control Policy

Whilst the principle of confidentiality necessitates that information is not made available or disclosed to unauthorised individuals or entities, the equally important principle of availability requires that information is available for use to the persons requiring said use. Therefore, at the company we have devised access controls which serve to establish an individual’s level of access to information, in turn ensuring that unauthorised individuals are not granted access.

Access management is not limited to access to information of the company, but additionally, and non-exhaustively, to premises, resources, networks, network services and equipment.

Access, physical or otherwise, shall be granted, revised, reviewed, and removed at the discretion of the Information Security Department.

In the table below, roles are provided with their respective level of access rights.

Role	User Admin	Security & Roles	Player Admin	Games	Payments	Bonus & Promotions	Site Content
Super Admin	Full	Full	Full	Full	Full	Full	Full
Admin	Full	View Only	Full	Full	Full	Full	Full
Operations	View Only	None	Limited	Limited	Limited	Full	Full
Payments	None	None	Limited	View Only	Full	View Only	View Only
Content Manager	None	None	None	Limited	None	Limited	Full
CRM Manager	None	None	Limited	View Only	None	Full	Full
Customer Support Manager	Limited	None	Limited	View Only	Limited	Limited	View Only
Customer Support Agent	None	None	Limited	View Only	Limited	Limited	View Only

User Management

The assignment of access to users shall be on a need-to-know basis and need-to-use basis. Certainly, the determination of the needs being linked to their roles as established in the Human Resources Roles & Responsibilities and the level of access, physical or otherwise, required by them for the proper performance of their job responsibilities. When granting access to a particular user, the company will factor the risk of lack of insufficient traceability and lack of insufficient confidentiality of information.

Information

Optimal management of information security necessitates that in information is classified depending on sensitivity and criticality, and which in turn establish the level of confidentiality required for that particular class of information.

At the company we have adopted the below classification of information:

Critical: This classification is to be assigned to information where incorrect information or disruption in processing of the information could result in substantial expense, embarrassment to the company, a violation of the law, or impairment of operations.

Sensitive: Sensitive information can be shared internally but not externally and will be adequately secured.

Public: Public information, such as advertising and marketing materials, is information that has been declared public knowledge by someone with the authority to do so and can freely be shared externally. When determining which class is best suited for a piece of information, due consideration of the consequences that a breach of confidentiality would cause, ranging from high to medium to low to nil. Consequences to be considered would be trust impact, financial impact, and legal impact.

Due to the 'Critical' class of information carrying most consequences in case of a breach, information which falls under this class are logs, personal data, business sensitive information and intellectual property.

Information shall be encrypted, and the more confidentiality-sensitive information shall be authenticated by measures such as digital signatures.

Requests for information which are genuine, authorised and not in violation of this policy, the law or other agreements are sent via an encrypted connection.

Non-electronic Critical and Sensitive information shall be filed in lockable storage, to which access shall be restricted to individuals who must have access on a need-to-know and need-to-have basis.

Generally, at the company we embrace a clear desk and clear screen policy, and all individuals are required to collect printed material from printers immediately. Computers shall be locked automatically after a short period of inactivity.

Non-electronic information which is not needed shall be shredded and disposed of accordingly. Electronic information, whether on fixed or removable storage devices, which no longer needs to be retained in terms of the Retention Policy or which is no longer needed shall be disposed of in a method instructed by the responsible Key Person as the method least vulnerable to potential security violations.

Any digital information in the critical and sensitive data category, whether on external drive, CD/DVD, or located on a computer hard drive, will be completely erased, and rendered unreadable. Obsolete computer equipment that is not beneficial to the company anymore may be internally sold or disposed. Old computer equipment may still hold residual information and/or software. If computer equipment is to be recycled, then all residual data must be removed beforehand. In case of equipment that has company information stored electronically, special care needs to be taken to wipe off the data in a way that it cannot be recovered using special tools and techniques.

Physical Access

Physical access to the server location centre is limited to access on a need-to-know basis.

Unaccompanied access to the server rooms is not permitted. Access to the server rooms is only granted to a few numbers of employees and to the CGA when requested or necessary.

Authorisation levels and access rights to company offices and server rooms are administered and approved by the responsible Key Person.

All employees shall be supplied with an access card, limited in accordance with the need-to-have-access principle corresponding to their role at the company. All camera-monitored areas shall have signs to adequately inform visitors that monitoring is in process, and employees shall be informed at pre-employment stage of the same. Records of security cameras shall be accessible in a sensitive manner in terms of this Policy and maintained and disposed in terms of the Retention Policy and general data protection legislation.

Visitor access shall be controlled to the extent that that visits may only be made for Company-related matters, and visits must be approved by the Information Security Department in advance of the visit who must also be informed of the purpose of the visit. Upon entry, visitors shall supply an identification document and shall be always accompanied by a Company employee in order that no access card would need to be given to the visitor. Visitors shall be recorded in a logbook to be maintained for the purpose, which log shall take note of the entry and exit times.

This information-security policy extends beyond the office/employee/head office/headquarters of the company due to the location of the servers and the hosting of information thereon. Access by third parties being employees of the hosting company shall be limited in terms of this Information Security Policy in the Service Level Agreement between the company and the Service Provider.

Certainly, access by representatives of the CGA as and when required shall not be limited.

Training And Responsibilities

Joiners, Movers, Leavers

At pre-employment stage, employees shall be provided with an Employment Contract to which there shall be attached a non-disclosure agreement the terms of which shall extend beyond date of termination of employment, for a set number of years which shall not be less than five (5) years.

Employees who change department shall have their access rights reviewed at the time of the change, to ensure that old access rights are removed and replaced with new ones, or alternatively that they are amended to reflect their new role and revised need-to-know and need-to-use levels.

At termination of employment stage, individuals are to return their access cards, any portable devices supplied to them together with any other company assets. Access rights will be terminated for employees who are terminated.

Third Party Service Providers

Service Level Agreements shall be drafted or vetted with maximum consideration afforded to the principles of information security established in this policy, as it would be futile to regulate information security within the company's organisation and fail to regulate appropriately the confidentiality of information and other Gaming Corps assets, which under such agreements would be in the hands of or accessible by third parties. Additionally, Service Level Agreement shall provide that the

confidentiality shall extend beyond the termination of the service, for a number of years or indefinitely, and moreover shall provide for the destruction of information.

VPN Remote Access

Restricting remote access to the company' individuals is crucial to minimise the risk on information security.

It is acknowledged that in order to maintain high productivity operations at the company, it may be required to grant non-managerial individuals' remote access. Such grants shall be on a strictly ad-hoc basis and decided upon by the management and the responsible Key Person with due consideration to urgency and necessity of remote access. The responsible Key Person may verify the remote connection before access is approved to ensure against threats and vulnerabilities.

Inactivity for fifteen (15) minutes shall automatically time-out a remote session.

Remote access shall be granted to authorised CGA representatives on request and if necessary.

Password Management

Everyone shall be assigned a User ID and shall be required to assign a password to his User ID in terms of the User Management Policy. Usernames and passwords must not be shared by users. Passwords must consist of at least 8 alpha numeric characters that must contain at least an uppercase letter, a lowercase letter, a number, and a special character and should not be written down.

The log-in system shall prompt users to change their password every thirty (30) days, and access shall not be granted in default.

Three (3) failed password attempts shall revoke access to the User, who is to notify the responsible Key Person of the matter for resolving.

Equipment, Devices, Media

Company personnel are supplied with a desktop working station as well as with portable devices such as laptops, tablets, mobile phones, and external storage devices, depending on their grade at the company. Such equipment and devices are considered the property of the company, and under no circumstance may they be used for non- Company -related matters. Suspected misuse of the equipment and or devices is to be reported to the responsible Key Person who is responsible to investigate and act if necessary.

Whilst Company equipment and devices are subject to regular maintenance to ensure against threats to confidentiality, faulty or malfunctioning equipment must immediately be reported to the Technical Officer who in turn, and if data confidentiality may be at risk, shall notify the responsible Key Person. Faulty or malfunctioning Company devices shall require that the same procedure is followed, and in no circumstance, may the individual have the portable device repaired by a third party.

The responsible Key Person is to be informed without delay of the loss or theft of any device to minimise potential unintentional disclosure.

Personal Devices

The access to Company information on a personal device shall be granted on a case-by-case basis for reasons established in 'VPN Remote Access'. Whilst this restriction does not apply to management, who it is understood must have freer access to Company information, the management must ensure that faulty or malfunctioning personal devices are brought to the attention of the responsible Key Person before repairs, in order that stored information is backed up or wiped out accordingly.

The Company only allows the use of removable storage media devices in instances when large amounts of information need to be shared internally or externally. In these cases, the following requirements need to be met:

- Approval needs to be obtained from the responsible Key Person
- Data can only be stored in a Company provided storage device.

Employees who are not supplied with Company-owned mobile handsets, tablets or laptops might require remote access to the Company email account, calendar, and contacts. Authorization to connect their personal mobile devices to the company servers must be requested from the responsible Key Person and the following requirements apply:

- Users are only able to access internal e-mail, calendar, and contacts. Any other service cannot be accessed through personal devices.
- Adherence to the best practice security measures.

If hardware, including servers, routers, firewalls, switches, hubs, storage or backup devices, must be decommissioned to undergo repair or maintenance, the responsible Key Person shall ensure that back-up is guaranteed and wiping out complete, before the procedure established in the Change Management Procedures is carried out.

Faulty or malfunctioning and beyond-repair media and equipment are subject to destruction, which is entrusted to the responsible Key Person, who is required to record all instances of destruction of media and equipment. Exceptions to this policy may be applied if it is determined that equipment may be put to use, albeit not for Company' purposes, provided that a wipe-out is affected beforehand.

For the proper implementation of these policies, all employees shall be informed of the content of this policy, and of any amendments thereto.

Network Security

The network is protected by means of firewalls, passwords, VPNs, and adequate encryption.

Network Security

The network is divided into zones guarded by VLAN configurations.

DMZ

The DMZ zone is protected by the (network/firewall).

All the application servers use HTTPS only to connect with clients.

All VLANs are routed via Firewall with restricted policies.

Remote Access / Management

Remote access to the system for management is only allowed for users that have been issued unique per-user client certificate to the VPN service.

User groups

Remote access can be granted with granularity, restricting a user to only be allowed to access servers and services the user has been granted clearance for.

Application Protection

All internally developed applications must be in accordance with security best practises and international standards. Such applications need to be properly documented and proper risk assessments carried out before being deployed and such deployment needs to be approved by the responsible Key Person. Access to all monitoring and control applications is to be secured by user authentication and should be limited by internal network access only.

Access to critical operational applications is to be secured through user authentication and network access. A redundant implementation of such applications must be deployed to ensure maximum availability. User actions are to be tracked within the application environment.

Every user of the back-office systems, regardless of access rights or role, has a mandatory 30-minute activity rule applied to their account. Specifically, this means that if a user's session is inactive for 30 minutes, their session will be automatically terminated. When the said user tries to use the back-office system again after this timeout, s/he will be prompted to login again and will start a new session upon successful login.

Security Awareness

The IT Team has installed the necessary antivirus and antimalware protection for the purpose of protecting against computer viruses, spyware, and other security threats to prevent, detect and clean-up. The Company shall also use intrusion detection and intrusion prevention systems to eliminate or minimise the risk on unwanted access to company network from the outside. To ensure the security of our IT environment, the following must be adhered to by all employees using company computers or systems:

- All computers accessing company systems must use the approved anti-virus protection software and configuration.
- The virus and firewall protection software must not be disabled or bypassed.
- The settings and automatic update frequency for the anti-virus software must not be altered in a manner that will reduce its effectiveness.
- Employees should never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source.
- Employees should never download files from unknown or suspicious sources.
- Employees should never complete any forms accessed via links embedded in an email from an unknown, suspicious, or untrustworthy source.
- Suspected viruses must be reported immediately to the responsible Key Person to ensure that adequate steps are taken not to compromise Company's data.
- The exchange of critical or sensitive information shall be encrypted.