

JORJAR SAC BUSINESS PLAN

Contents

1. Company Summary	3
1.1. Product and Services	3
1.2. Market Situation	3
1.3. Marketing Strategies	4
1.4. Company Structure and initial organization	6
2. Financial Plan	7
2.1. Funds Management	7
3. Technical & Product Details	7
3.1. Products & Services	7
3.2. Technical Infrastructure	8
3.3. Application Architecture	8
3.4. Applications	12
3.5. Network Architecture	12
3.6. Backup Procedures	12
3.7. Backup Restore Testing Plan	14
3.8. Business Continuity and Disaster Recovery	15
4. Policies	26
4.1. System Access Policy	26
4.2. User Management Policy	29
4.3. Change Management Policy	32
4.4. Financial Accounting Policy	36
4.5. Fraud Management Policy	37
4.6. Information Security Policy	37
4.7 Incident Response Plan	43

1. Company Summary

This document seeks to develop a business plan pursuant to establishing an online wagering site under the Curaçao eGaming licence jurisdiction. The object of the site will be to provide entertainment to its users in a safe and reliable manner.

Currently, there are a wide variety of sites that offer entertainment and online casino services, due to the exponential growth of the industry as a result of the current global pandemic. However, many of those sites do not have a licence, certification or a regulatory system that governs them, directly affecting the customer's decision to gamble. It is those organisations that provide security to the players, since they have the objective of regulating fair play, money laundering, and have minimum legal requirements to provide a safe and legal online casino technology platform. As a company, we will provide a service that offers the necessary guarantees to the players to establish gaming options that are fair play and, above all, legal.

1.1 Product and Services

Our product consists of the creation of an online betting web platform, which offers entertainment services to users, providing security and trust guarantees through the Curaçao eGaming licence. Its objective is to certify fair play, in addition to security and the recognition of an organisation with more than 20 years in the market.

The website will feature games of chance such as slots, roulette, virtual games, and online sports betting. The platform will allow the creation of individualised users for each client, so that they can carry out a more efficient and secure payment process, collecting their bonuses and prizes through the personal accounts of each user.

1.2 Current Market Situation

The online casino platform will reach people who seek entertainment through the online gambling and gaming market in order to generate extra income through gambling.

It will seek to attract the attention of gamblers, men and women of legal age, who have internet access and seek entertainment through online gambling, by means of our website. We will apply a demographic segmentation, which aims to encompass most of the customers we seek to attract to this type of service.

The needs of each client can be varied at the time of generating a bet through the internet, and these will depend on each person, since many wager as a hobby, entertainment or way of life. Each bettor seeks a different objective when choosing an online casino platform, and they may prefer those sites that give them greater benefits or choose the site that gives them greater confidence, among other preferences. Therefore, it is necessary to generate a website that can accommodate a large part of

those needs and thus provide a platform that encompasses a large part of those requirements, which is safe, reliable, and attractive.

With regard to the casino industry, the pandemic has led to restricting the mobility and operation of different companies worldwide, due to the sanitary measures imposed by the authorities of each country, affecting or favouring the operation of the different types of existing industries. However, it is those measures that have caused a positive impact on the online services industry, which is our responsibility, among other things, due to the difficulties in opening physical gambling halls in different Latin American countries, causing customer portability towards web platforms.

1.3 Marketing Strategies

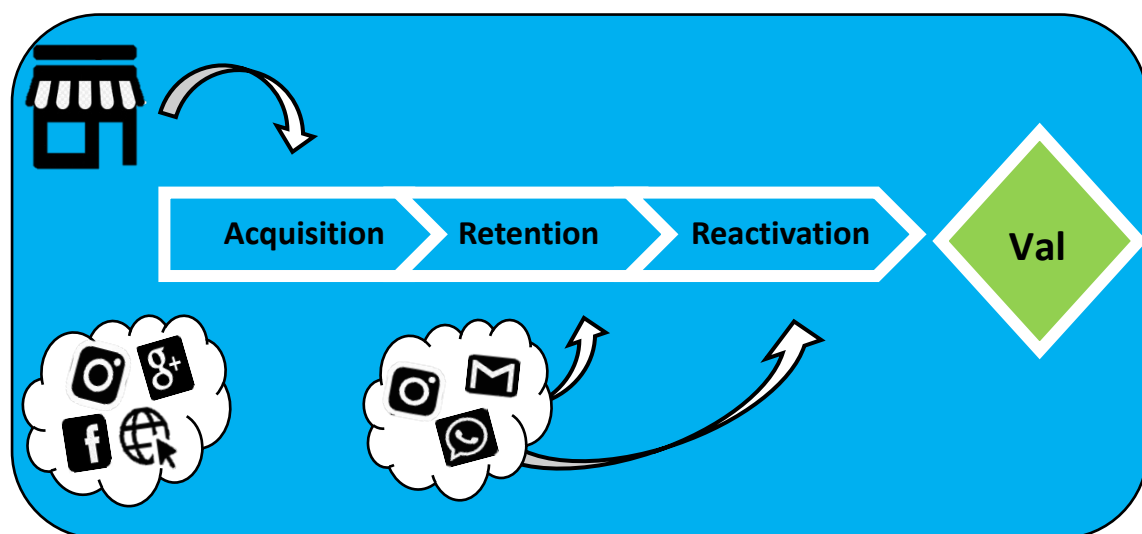
The company will develop and conduct marketing strategies, both land-based and digital.

Offline Marketing:

Advertising will be done through posters and banners with information and promotions that motivate the client to visit the platform, in different centrally located venues with a high flow of people.

Digital Marketing:

We will conduct marketing actions through different digital channels that allow us to meet our clients in a timely manner, taking advantage of the strong global penetration that social networks have had in the current global pandemic scenario. The strategies to be implemented have the objective of covering the greatest number of potential clients, in addition to generating a close and personalized relationship with the client. That said, a design is used in the marketing process which is divided into: ACQUISITION - RETENTION - REACTIVATION. Using the different channels applied in each stage of the process.



a. Customer acquisition:

Social networks will be used in general, emphasising Facebook and Instagram as channels for mass advertising and customer contact, since each of the profiles will lead to our official website and our Contact Centre for more information. The main objective of this medium is the generation of content related to the business, promotions, and diverse information in order to make people aware of our brand and the online casino website. It is also expected to have the participation of influential people in order to motivate and generate more visits to our site and reach more potential clients through promotional codes. Additionally, we expect to invest in paid advertising on Facebook and Instagram in order to reach the expected segmentation and market niche. In short, the use of social networks will mainly contribute to attracting customers, together with the implementation of web positioning within the Google search engine and thus obtain a privileged position within the search engine with respect to the competition so that the customer finds access quickly to the website.

b. Retention:

Email marketing will be used as a channel for customer loyalty along with Instagram and WhatsApp. WhatsApp will also be used as a means of communication between the client and our Support centre, in order to generate a close and timely relationship with their requirements. It will be through this channel that the client will be able to make customer service inquiries, support claims, or redeem various promotions related to the games, delivering an efficient and fast service in order to satisfy the players with a quick response time. Influencing directly on CUSTOMER SATISFACTION, since they will be private channels of communication and with a personalised treatment. Likewise, the use of email together with WhatsApp will be for the purpose of carrying out campaigns to the different users with exclusive offers for each of them and special promotions, with the aim that the client feels VALUED in the delivery of benefits according to the specific customer tier, and even a bonus coupon on their birthday. All this in order to retain the customer so they will continue to use our platform.

We will have our active clients segmented by gaming volume, which will allow us to deliver differentiated stimuli according to the particular profile of each client.

c. Reactivation:

For those customers who do not access our site for certain periods we will use strategies of evaluation of loss of the prospect. It will be through different means of communication that we will obtain the customer's opinion and subsequently stimulate it with different incentives configured according to the profile of the target customers. In turn, email and SMS campaigns, among other channels, will be used as means of contact to recover customers with low activity or inactive rates, where they will be objectively advertised to in a personalised manner so that they visit and use the Website. Also considered for those who are inactive is to offer temporary or expiring promotional codes to encourage the use of the web platform.

WhatsApp will also help in sending special promotions to each client belonging to our database, in order to encourage them to use the web platform.

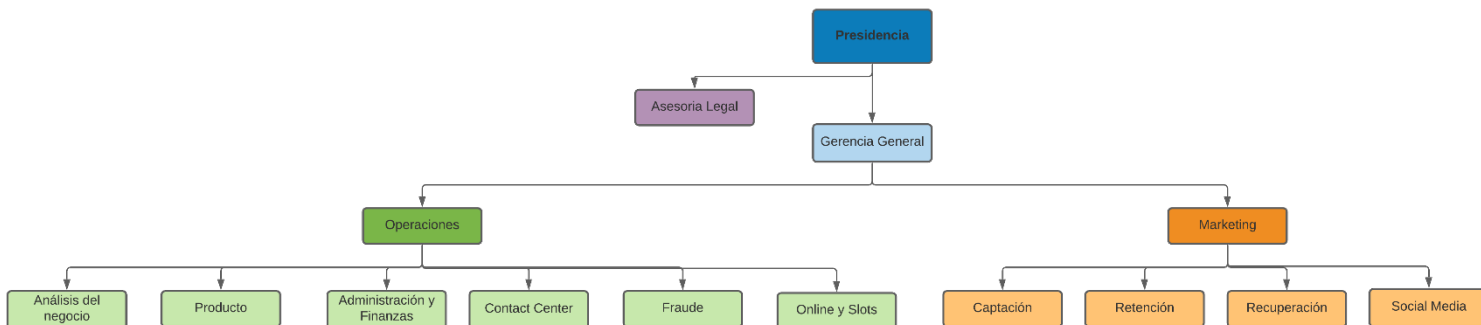
1.4 Company Structure and initial organization

The business was formed through a company made up of those who today make up the directorate of the organisation. This has the objective of providing an entertainment space through the assignment of responsibility channelled through the different existing departments within the business, which allow to fulfil the main objective that the company wishes, through collective and synchronised work.

1.4.1 Organizational chart

As the graphic representation of how our organisation is composed at its different levels, that is, how the company is organised, being in this particular case in a hierarchical manner.

Our organisation applies a vertical organisational chart, this type of structure being one of the most commonly used, due to the order of the pyramid that it has (at the highest levels we find those who have greater authority). This type of distribution allows greater benefits in the administration of the company, due to the clarity of functions, limitations of responsibility and communication channels.



1.4.2 Roles and responsibilities

For the correct operation of the company, it is necessary to describe in detail the functions and positions that each one of its members will have in order to work in an orderly and coordinated manner, since they establish the responsibilities and tasks of each one of the collaborators belonging to the organisation.

A. President:

The company is organized through a general presidency whose responsibility is to make structural decisions for the company.

B. General Management:

The general management is responsible for leading the company to guarantee the operational continuity and viability of the business.

C. Operations Management:

This role is in charge of compliance control and optimisation of operational processes inherent to the business.

D. Marketing Management

This department is in charge of conducting those strategies that maintain the presence of the company in the market and develop effective communication with customers through Acquisition – Retention and Reactivation. All of the above, is through the different campaigns generated by this department.

2 Financial Plan

2.1 Funds Management

	Year 1	Year 2	Year 3
Total Revenue	US\$ 225,000	US\$ 10%	US\$ 10%
Total Expenses	US\$ 30%	US\$ 30%	US\$ 30%
Net Result	US\$ 75,000	US\$ 90,000	US\$ 99,000

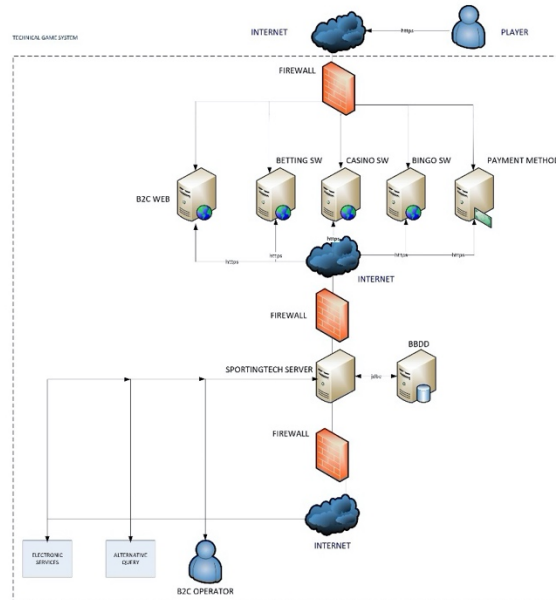
3 Technical & Product Details

3.1 Products & Services

- Online sports wagering
 - Pre-match sports betting
 - In-play sports betting
- Online Casino table and slots games
- Live Casino

- Virtual sports wagering

3.2 Technical Infrastructure



3.3 Application Architecture

The applications currently being used by JORJAR are the following:

- Casino & Sports Frontend Service
- Casino Engine
- Casino API
- Casino Back Office Application
- Odds Preparation Services
- Live Odds Distribution Services
- Prelive Odds Distribution Services
- Sports API Services
- Sports Back Office Services
- Sports Retail Services
- Nginx Services
- Payment Gateway API Services
- Master Database
- Sports Odds Master Database
- Sports Odds & Transaction Slave Database
- Sports Transaction Master Database
- BI Master Database

- BI Slave Database
- Casino Transaction Master Database
- Casino Transaction Slave Database
- Transaction Backup Database

3.3.1 Casino & Sports Frontend Service

The Frontend Service is mainly to manage the front facing portal in use by players. The applications used for this function are:

- a) Customer Registration
- b) Wagering
- c) Deposits, Withdraws and Game reports

3.3.2 Casino Engine

Casino Engine is the connector between JORJAR and Casino vendors. Every transaction processed in this application is recorded in the Database.

3.3.3 Casino API

Casino API is the connector between casino services and sports services used for processing open game, balance enquiries and deposit from/to casino balances.

3.3.4 Casino Back Office Application

The casino back office application is used to manage players as well as operational risk.

The main functions handled by the Casino Back office Application are:

- a) Risk Management
- b) Game Setup
- c) Customer KYC
- d) Deposits and Withdraws
- e) Reports
- f) Bonus Management
- g) Financing

3.3.5 Odds Preparation Services

Odds Preparation Service is used for creating trader-based odds data from the raw rates provided by the odd providers and trader based configuration data.

3.3.6 Live (in-play) Odds Distribution Services

Live Odds Distribution Service is implementing the websocket technology where the web frontend users are experiencing in-play odds during the games.

3.3.7 Prelive Odds Distribution Services

Prelive Odds Distribution Service provides the odds for the upcoming games before they start.

3.3.8 Sports API Services

Sports API Service is at the center of all API services ranging from user authentication up to coupon creation and completing betting services.

3.3.9 Sports Back Office Services

Sports Back Office Service is a dashboard, used by traders, which provides the configuration functions for their web sites. The main functions handled by the Sports Back office Application are:

- a) Risk Management
- b) Game Setup
- c) Customer KYC
- d) Deposits and Withdraws
- e) Reports
- f) Bonus Management
- g) Financing

3.3.10 Sports Retail Services

Reporting, odds distribution and API services used by retail applications.

3.3.11 Payment Gateway API Services

Payment Gateway API is the bridge between JORJAR and 3rd party payment vendors which JORJAR is working with. The main functions of the application are:

- a) Deposits
- b) Withdrawals

3.3.12 Nginx Services

Nginx Services (consisting of Nginx or NGINX+ software) are the user entrance point to frontend or API endpoints. Caching, access management, proxying, load-balancing, performance management and monitoring are fulfilled on Nginx Services.

3.3.13 Master & Slave Databases

This is where all the information regarding registered players, player gaming transactions, player history, un-rated and rated odds are recorded. The Master Database is also used to generate any reports required.

3.3.14 Sports Odds Master Database

Used for storing raw odd data provided by the odd providers.

3.3.15 Sports Transaction Master Database

Used for storing rated odds, registered players, player gaming transactions, player history and all type of financial transactions.

3.3.16 Sports Odds & Transaction Slave Database

Realtime replica of odds & transaction master databases.

3.3.17 BI Master Database

Used for storing historical player & betting data.

3.3.18 BI Slave Database

Realtime replica of BI master database

3.3.19 Casino Transaction Master Database

Used for storing casino game transactions.

3.3.20 Casino Transaction Slave Database

Realtime replica of casino transaction master database.

3.3.21 Transaction backup DB

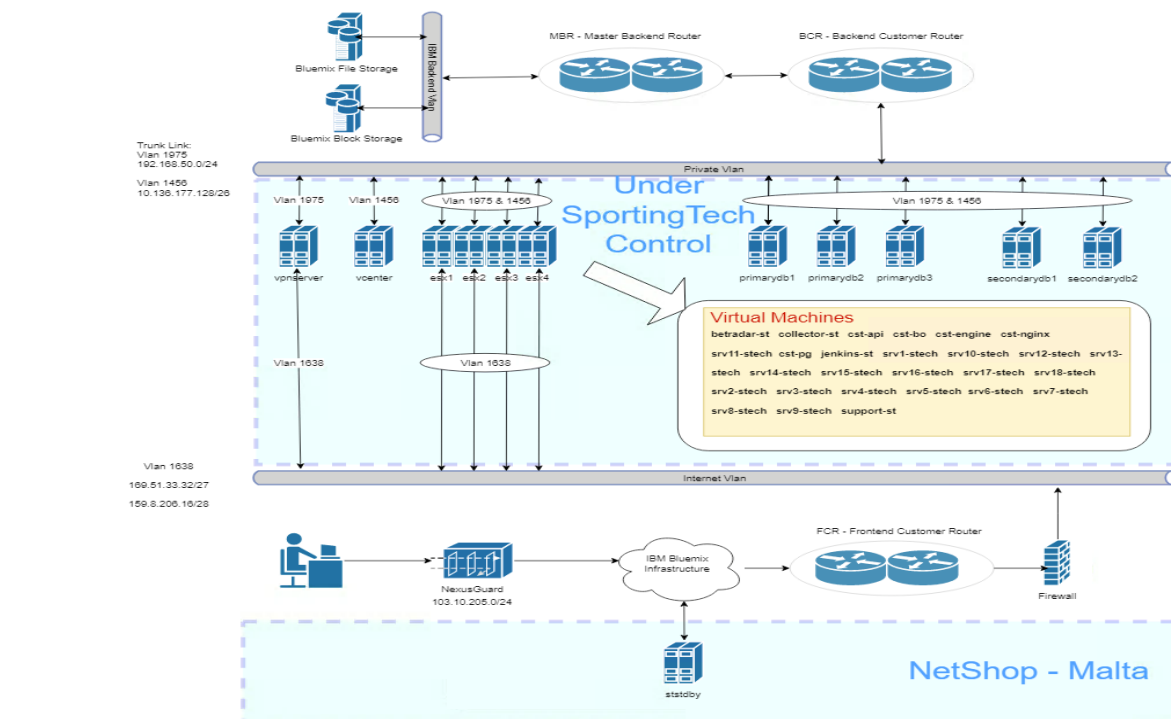
Used for storing financial transactions & bet data for both casino & sport services. It is used as the backup database of casino.

3.4 Applications

The online gaming platform will provide users with sports betting and Casino game options for:

- Desktop format
- Mobile format

3.5 Network Architecture



3.6 Backup Procedures

This document outlines the backup procedures carried out by JORJAR Ltd with the aim of formalising this process.

3.6.1 Objectives

This document aims to protect JORJAR Ltd customer sensitive data in case of any system disk drive or equipment failure, corruption of data, or major disaster. In such cases, this document ensures that no data will be lost and would be fully recoverable. The backup procedure covers only customer sensitive data.

3.6.2 Responsibilities

The data backup procedure will be overseen by the Information Security (IS) Manager, who ensures that this procedure is being successfully carried out. The IS Manager is also in charge of periodically reviewing this procedure and ensuring that periodical restore testing is being carried out.

3.6.3 Policy

3.6.3.1 Backup Process

Any customer sensitive data is backed up regularly in order to restore data in case of a system failure which requires full restoration of data.

3.6.3.2 Naming Convention

A file naming convention must be employed to clearly distinguish between those files used for production purposes and those files used for testing or training purposes.

3.6.3.3 Backup Schedule

Data on the server is being continuously backed up using a RAID configuration which mirrors the data being stored in real time. This is the best way to ensure that the most up to date information is available in case of an incident. Backups include all gaming data, transaction data and system.

Furthermore, data on primary database node is being backed up to the secondary database node in real-time. This ensures that in the worst case scenarios, Sporting Tech Software does not suffer a large loss of data.

3.6.3.4 Website backup

Every version of the website site is securely archived whenever a change is implemented to ensure a rollback is possible in case of an incident. JORJAR Ltd is using Apache Subversion and Git for source code backups.

3.6.3.5 Firewall backup

JORJAR Ltd is using Linux based firewalls, with its configurations fully backed up immediately after deployment and regularly thereafter.

3.6.3.6 Portable Computer Backups

JORJAR Ltd does not encourage the retention of sensitive information on laptops, however if there is a business need for storing such information, the employees who make use of this portable device must make regular backups.

3.6.4 Offsite Backups

Essential business information and information relating to player data are being replicated in disaster recovery site.

3.6.5 Backup Restoration and testing

Restoration tests are carried out on the test environment to ensure that data can be restored every six months.

Should there be any critical business information or critical software which has been archived on computer storage media for a prolonged period of time; this must be tested at least annually.

Logs are kept to record these restoration tests.

3.7 Backup Restore Testing Plan

The objective of this policy is to ensure MGS is protected against loss (availability) or corruption (integrity) of data and services and to ensure continuity in service delivery.

3.7.1 Backup is the process of copying data (ITIL).

3.7.2 Restore is returning a Configuration Item or an IT Service to a working state. After Recovery, further steps may be needed before the IT Service can be made available to the users (Restoration). (ITIL)

3.7.3 Backup Strategy is a strategy, applied to the process of backup, regulating various parameters, like how much data is backed up at a time, how often backup is performed, and which media is used. A backup strategy usually aims at achieving both effectiveness and efficiency at the same time, in other words combining the best security with the least efforts and costs.

3.7.4 Restores and restore times must be tested according to the restore test schedule, i.e. one restore test per site per month are done on randomly selected DB's

3.8 Business Continuity and Disaster Recovery

To ensure that the organisation is able to continue its commercial activities in the event of significant disaster scenarios.

3.8.1 Objectives

This document ensures that JORJAR Ltd data, hardware, and software are saved so that critical processes can be resumed in the least time possible, and have data restored in order to continue with the operation.

3.8.2 Responsibilities

Staff responsible for ensuring this procedure is carefully followed and executed in case of a disaster, are the Information Security Manager, Key Function for Technological Affairs, Key Function for Network and Information Security, and Senior Management. Senior Management includes the Board of directors and the Chief Executive Officer who will be taking the crucial decisions relating to JORJAR Ltd operation.

3.8.3 Policy

All critical business applications, processes and infrastructure must have a documented, current, and regularly-tested contingency plan that permits the restoration of service within 72 hours.

JORJAR Ltd ensures that responsibility for managing and facilitating the restoration of service is clearly laid out, and employees receive sufficient training and practice to permit them to follow these same procedures to help successfully restore the affected service.

3.8.4 Scenarios and Mitigation plan

3.8.4.1 Power Failure

Loss of power normally isn't a matter of urgency, since both the office and the data centre are equipped to cope with such a scenario.

The staff on duty are asked to check how long the power shortage is expected to take, however it is out of JORJAR Ltd control. This scenario would pose a problem in cases of prolonged power failure.

3.8.4.2 Internet/Network Failure

In case of problems with or the loss of network connectivity resulting in players being unable to enjoy the gambling experience, for outages which may take more than 12 hours, traffic will be temporarily redirected to the disaster recovery site with limited functionality until the problem is resolved.

If this solution is not possible, players would be redirected to a website hosted outside of primary datacenter (DC), which does not contain any gambling related material, but however informs the players that the website is experiencing technical difficulties.

This problem will normally result in downtime of maximum two hours until any configuration changes are made and propagated.

3.8.4.3 Loss of data / Server / firewall

Should there be a problem with the database server or any other server, JORJAR Ltd has set up redundant servers to mitigate such a problem in a short time by swapping the servers until the problem can be rectified. Once repaired hardware is installed back on the live system it will be made available as the secondary server.

Remediation of the problem depends on the type of problem. This operation is normally expected to take not more than two hours.

3.8.4.4 Unauthorised Server Access / Security Breach

Should JORJAR Ltd be aware of unauthorised access, the information security department needs to first of all carry out the following tasks:

- i. A full scan of the network is carried out to see if any malicious programs or viruses and other back-door applications have been intentionally installed
- ii. Passwords are changed and made more secure
- iii. Data integrity is verified to ensure that no tampering has been made to the data
- iv. Audit logs are reviewed together with any changes made to see what areas have been breached

Finally, a report is issued to see how the attacker bypassed the security mechanisms and what can be done to prevent future occurrences of such an incident.

3.8.4.5 Major Disaster resulting in loss of Office Space

Employees are trained to be able to cope with the restoration of normal business activity after an emergency or a disaster disrupts business activity.

JORJAR Ltd regularly involves employees in off-site recovery operations, where employees are asked to work from outside the office in order to be prepared for such a scenario.

In case of a major incident/disaster resulting in the loss of office space, staff can therefore connect remotely to the system in order to be able to carry out their work. Telephone Customer Support would have to be halted until new office space is established and set up, however chat and e-mail support would still be available to the players.

This process can take up to a month; depending on how quickly an alternate office is found.

3.8.4.6 Major Disaster resulting in loss of Data Centre

In case of a disaster resulting in the loss of the Data Centre, recovery from the loss will be conducted in a three-phased approach. Critical systems and applications will need to be effectively and efficiently recovered in order to continue the business in the least time possible.

Phase I of the recovery process involves moving the operations to the Disaster Recovery Backup Site, which is also located in the JORJAR Ltd in one of JORJAR Ltd data centre, but in a different location. There is a targeted period of up to 48 hours for staff to set up the backup site.

Phase II of the recovery process involves recovering the critical business functions, restoration of the critical applications and critical network connectivity. The backup site has replicated data from the primary site, and therefore switching to the alternate site should not pose much of a problem.

The aim of this phase is to recover the systems and network as quickly as possible so that the website is back online, and players can continue making use of the portal.

Phase III of the recovery process is having all the data processing activities transferred back to a primary Co-Location Facility, once it has been re-established.

3.8.5 Business Impact Analysis

In each of the above scenarios, a business impact analysis (BIA) is performed before recovery is attempted. The BIA will determine what needs to be recovered and how quickly.

It is very important to conduct this process diligently since any recovery plans will be built on this assessment. The BIA helps senior management identify how the operation was affected following a disaster and also to help set a budget (if needed) to recover from the disaster.

3.8.6 Testing of BCP

This plan is periodically updated, and tested regularly to ensure that JORJAR Ltd would be prepared and would be able to continue operations in the event of a business interruption.

3.8.7 Escalation

In each scenario, the Information Security Manager should be made aware of the situation. The CEO, Key Function for Technological Affairs, and Key Function for Network and Information Security will also be notified so that they can intervene if necessary. For major disasters like loss of office space and loss of Data Centre, the Board of Directors will also be kept informed.

3.8.8 Appendix A – Contact / Escalation List

Name	Position	Contact Number

3.8.9 Appendix B - more possible Disaster Scenarios and Recovery Strategies

Hardware Failure

Scenario	Single Hard Disk Failure
Effect on Operations	None
Impact Level	None
Possible Cause	Hardware Fault
Action	Replace and order a new one. RAID set up will make another disk take over. Up to 2 days to get a new disk.
Responsible Person/s	Information Security Manager
Time to resume normal operation	Worst Case Scenario - 2 days

Scenario	Other Hardware Failure (e.g. power supply, processor, memory)
Effect on Operations	None

Impact Level	None
Possible Cause	Hardware Fault
Action	Replace and order a new one
Responsible Person/s	Information Security Manager
Time to resume normal operation	Immediately

Scenario	Failure of Network Devices
Effect on Operations	None
Impact Level	None
Possible Cause	Hardware Fault
Action	Replace and order a new one. All network devices have full failover. Up to 2 days to get a new Device.
Responsible Person/s	Information Security Manager
Time to resume normal operation	Worst Case Scenario - 2 days

Scenario	Failure of Firewalls or Switches
Effect on Operations	None
Impact Level	None
Possible Cause	Hardware Fault
Action	Replace and order a new one. All network devices have full failover. Up to 2 days to get a new Device.
Responsible Person/s	Information Security Manager
Time to resume normal operation	Worst Case Scenario - 2 days

Power Outage

Scenario	Power Supply Outage
Effect on Operations	Data Centre have backup for this, through batteries and gasoline generator
Impact Level	None
Possible Cause	Many..
Action	Automatic failover

Responsible Person/s	Hosting provider
Time to resume normal operation	Immediately

Scenario	Single Server Power Outage
Effect on Operations	More load on other servers
Impact Level	Minimal
Possible Cause	Hardware fault
Action	Replace. Up to 2 days delivery.
Responsible Person/s	Information Security Manager
Time to resume normal operation	Worst Case Scenario - 2 days

Data Centre Outage

Scenario	Data Centre Outage
Effect on Operations	Downtime for up to 10 hours
Impact Level	Severe
Possible Cause/s	
Action	Backups needs to be restored on alternative location
Responsible Person/s	Information Security Manager
Time to resume normal operation	72 Hours

Application Failure

Scenario	Application Failure
Effect on Operations	Depends very much on what part of the application
Impact Level	Minimal
Possible Cause/s	Bad deploy
Action	Restart of servers or alternatively hot deploys might be needed
Responsible Person/s	Information Security Manager
Time to resume normal operation	2 hours

Data Loss

Scenario	Data loss of one of front-end or application servers
Effect on Operations	None
Impact Level	None
Possible Cause	Hardware failure
Action	Replace Hardware. 2 days to get a new one
Responsible Person/s	Information Security Manager
Time to resume normal operation	Worst Case Scenario - 2 days

Scenario	Data loss of all of front-end or application servers
Effect on Operations	Downtime till one or more servers have been recovered from backups
Impact Level	Severe
Possible Cause	Many
Action	Restore from Backup. Less than 3 hours.
Responsible Person/s	Information Security Manager
Time to resume normal operation	Less than 8 hours

Scenario	Complete Data Loss
Effect on Operations	Downtime till one or more servers have been recovered from backups
Impact Level	Severe
Possible Cause	Nuclear bomb, earthquake or similar catastrophe
Action	Restore from Backup if this exists anymore
Responsible Person/s	Information Security Manager
Time to resume normal operation	Unknown – depends on severity of damage suffered by the infrastructure

(D)DoS / Brute Force Attack

Scenario	DoS / Brute Force Attack
Effect on Operations	Slow response from servers
Impact Level	Minimal
Possible Cause	DDOS will be the cause..

Action	Monitor and inform DDoS protection service provider to also make them do necessary prevention of access to the network
Responsible Person/s	Information Security Manager
Time to resume normal operation	30 minutes

Office Internet Connectivity Outage

Scenario	Internet Connection Problems
Effect on Operations	Slow internet
Impact Level	Minimal
Possible Cause	ISP problems
Action	Use mobile internet or go to an alternative location
Responsible Person/s	Information Security Manager
Time to resume normal operation	Immediate

Data Compromise by External Sources

Scenario	Data Compromise by External Sources
Effect on Operations	NA
Impact Level	NA
Possible Cause	NA
Action	NA
Responsible Person/s	Information Security Officer
Time to resume normal operation	Unknown – Depends on the severity of the breach

Negative Media Exposure

Scenario	Negative Media Exposure
Effect on Operations	Weakened brand value
Impact Level	Depends
Possible Cause	Bad player handling
Action	Keep an open communication with media
Responsible Person/s	Chief Operating Officer

Time to resume normal operation	Immediate
--	-----------

Loss or Theft of Computer

Scenario	Loss or Theft of Computer
Effect on Operations	None
Impact Level	Minimal
Possible Cause	A thief
Action	Change passwords and renew computer. Contact the police
Responsible Person/s	Information Security Manager
Time to resume normal operation	Immediate

Head Office Infrastructural Damage / Building Loss

Scenario	Head Office Infrastructural Damage / Building Loss
Effect on Operations	It will be slow for a while
Impact Level	Minimal
Possible Cause	NA
Action	Relocate if needed
Responsible Person/s	Information Security Manager
Time to resume normal operation	Unknown - but can continue operating if data centre remains intact.

Head Office Break-in

Scenario	Head Office Break-in
Effect on Operations	Depends
Impact Level	Minimal
Possible Cause	NA
Action	Contact the police
Responsible Person/s	Information Security Manager / Chief Operating Officer
Time to resume normal operation	Immediately

Data Centre Infrastructural Damage / Building Loss

Scenario	Data Centre Infrastructural Damage / Building Loss
Effect on Operations	Depends on servers and equipment affected
Impact Level	Depends
Possible Cause	Depends
Action	Depends
Responsible Person/s	Information Security Manager
Time to resume normal operation	Unknown - but can continue operating if data centre remains intact.

Data Centre Break-in

Scenario	Data Centre Break-in
Effect on Operations	Depends on servers and equipment affected
Impact Level	Depends
Possible Cause	Depends
Action	Depends
Responsible Person/s	Information Security Manager
Time to resume normal operation	Unknown – depends on the damage the data centre sustains.

Deliberate System Compromise by member of staff

Scenario	Deliberate System or Data Compromise by Member of Staff
Effect on Operations	Depends on servers and equipment affected
Impact Level	Depends
Possible Cause	Depends
Action	Police
Responsible Person/s	Information Security Manager
Time to resume normal operation	Unknown – depends on the damage inflicted

Database Master

Scenario	Database Master Failure
-----------------	-------------------------

Effect on Operations	Slave will take over
Impact Level	Low
Possible Cause	Disk failure
Action	Investigate and do necessary replacements to get the master back up. Less than 3 hours to fix
Responsible Person/s	Information Security Manager
Time to resume normal operation	Less than 4 hours

Scenario	Database Slave Failure
Effect on Operations	None
Impact Level	Low
Possible Cause	Disk Failure
Action	Investigate and do necessary replacements to get the slave back up. Less than 1 day to fix.
Responsible Person/s	Information Security Manager
Time to resume normal operation	Less than 2 days

Scenario	Application Server Failure
Effect on Operations	None
Impact Level	None
Possible Cause	Hardware or bad deploy
Action	Investigate and get the server back up. Less than 3 hours to fix.
Responsible Person/s	Information Security Manager
Time to resume normal operation	Less than 3 hours

Scenario	Front-End Server Failure
Effect on Operations	None
Impact Level	None
Possible Cause	Hardware or bad deploy
Action	Investigate and get the server back up
Responsible Person/s	Information Security Manager

Time to resume normal operation	Less than 3 hours
--	-------------------

4 Policies

4.1 System Access Policy

The purpose of this policy is to outline access measures, which will be employed by JORJAR Ltd in order to protect the confidentiality, integrity and availability of all its information systems through the proper control of user access and minimise any risk resulting from unauthorised modification or access to those systems.

This document aims to prevent unauthorised access to JORJAR Ltd sensitive customer data by ensuring that users have access only to the information relevant to the tasks assigned to them.

This document applies to all employees and third parties who are making use of JORJAR Ltd information systems.

4.1.1 Information Security Manager

For the purpose of this document, the role of Information Security Manager will be responsible for protecting and safeguarding data, and managing access to the company's information systems.

The Information Security Manager will also be in charge of enforcing this policy and ensure that adequate training/advice is given to new staff who should be aware of the information security best practices and procedures as outlined in this and any other relevant documents.

4.1.2 Need to Know

Access to information must be provided based on the need to know. Information must be disclosed only to people who have a legitimate business need for the information. At the same time, workers must not withhold access to information when instructions were given for that information to be shared. To implement the need-to-know concept, JORJAR Ltd has adopted an access request and approval process. Staff must not attempt to access sensitive information unless the appropriate access rights have been granted to them.

When a member of staff changes their job duties, including; termination, transfer, promotion and long periods of leave of absence, his or her supervisor must immediately notify the Information Security department so access is reviewed for that particular individual. The privileges granted to all workers must be periodically reviewed to ensure that only those with a current need to know, presently have access.

4.1.3 Physical Security to Control Information Access

Access to every office, server room, or any other work area containing sensitive information must be physically restricted to those people with a need to know. When not in use, sensitive information must always be protected from unauthorised disclosure. The physical access to the servers on IBM are defined under IBM Cloud policies / procedures.

When an employee leaves a room unattended, they must ensure that sensitive information in paper form is locked away in appropriate containers or at least, they must ensure that all doors and windows to the unattended room are closed and locked.

During non-working hours, workers in areas containing sensitive information must lock-up all information. Employees must position their computer screens such that unauthorized people cannot look over their shoulder and see the sensitive information displayed.

4.1.4 Clear Desk Policy

Unless information is in active use by authorised people, desks must be clear and clean during non-working hours to prevent unauthorised access to information.

4.1.5 Third Party access

Unless it has specifically been designated as necessary, all JORJAR Ltd internal information and systems must be protected from access by third parties. Third parties may be given access to JORJAR Ltd internal information and systems only when a demonstrable need to know exists, when a non-disclosure agreement has been signed, and when such a disclosure has been expressly authorised.

If there is suspicion of unauthorised access to JORJAR Ltd information systems, or if sensitive information is lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed to unauthorised parties, the Information Security department must be notified immediately.

4.1.6 Third-Party access and information disclosure

Unless an employee has been authorised to make public disclosures, all requests for information about JORJAR Ltd and its business such as questionnaires, surveys, and newspaper interviews, must be referred to the person in charge of public relations. This does not apply to sales and marketing information about JORJAR Ltd products and services, nor does it pertain to customer technical support calls.

As a general rule, access to JORJAR Ltd systems by third parties is not allowed. However, access may be granted if they have a legitimate business need and shall only be given for the duration of the assignment.

4.1.7 Remote Access

As a general rule, remote access to JORJAR Ltd systems is only allowed to staff via VPN which requires 2FA (VPN certificate and username & password). Security measures are in place to ensure that the remote session is not vulnerable to attack; the connection has to be done through VPN.

Should there be the need of establishing a direct connection between JORJAR Ltd systems and computers at external organizations, through the Internet or any other public network, it must be approved by the Information Security manager.

4.1.8 Granting access rights

Any request for access to customer sensitive data must be made by team manager via a ticket, slack or in writing (by email or hard copy) and must include the following information:

Start Date of Employment	Day/Month/Year
Name of Employee	Mr/Mrs/Ms. Xxxxx
Job title of the new employee	Ex. Customer Care Executive
Occupational group	Ex. Customer Support
Contact details	Ex. Work: 123-456 Ext. 54 Personal: 123-456
Additional Access required	Ex. Customer Management, Issuing of Reports (By default, new accounts have access to the Microsoft Office Suite and Internet.

Access to new employees shall be granted as follows:

- The request is sent to the Information Security department either by the new employee's manager or by Human Resources, with the required information.
- The Information Systems Manager reviews the request and upon approval, the new employee's e-mail address and user account are created. Access is given as specified in the access request.

- The new user account will not however be available until the employee's start date. On the first day, the new employee will be advised of the user-id and password. The system will force them to change the password upon first login.
- The job title of the employee should be specified by the his/her team manager based on the table below aiming to sustain the segregation of duties.

Role
Senior Developer
Junior Developer / New Joiner
Application Support
Senior QA Engineer
Junior QA Engineer / New Joiner
Release Manager / Engineer
System Analyst
System Support Engineer

4.1.9 Revocation of access rights

When an employee leaves the company, Human Resources or employee's manager inform the Information Systems department of the employee's new employment status promptly in writing (slack, ticket or email). The IS department then deactivates the user's account and ensures that all privileges have been revoked.

4.1.10 Review of access rights

Access rights are re-evaluated regularly by management to ensure that no employees have more access rights than their need to know. Should an employee's role change, the Information Systems department should be informed beforehand so they can make the necessary changes to that employee's access levels.

4.2 User Management Policy

JORJAR Ltd makes heavy use of information systems, which is dependent on a user's activity. As a result, a large part of JORJAR Ltd.'s daily business involves the handling of sensitive information. To this end, this policy provides guidelines and instructions to all users who make use of these systems. All employees are expected to comply with this policy. Non-compliance with policies can result in disciplinary action up to and including termination.

The primary objective of the policy is to establish guidelines that will minimise unwanted user behaviour while using JORJAR Ltd.'s information systems.

4.2.1 Personal Use

JORJAR Ltd.'s information systems are intended to be used for business purposes only. Personal use is only permissible if it consumes a small amount of resources that could otherwise be used for business purposes and does not interfere with worker productivity.

Permissible use of e-mails would, for example, involve sending a message to schedule a personal appointment or paying a bill online. Games that are shipped with computer operating systems can be played during scheduled breaks or lunch as long as this activity does not interfere with either worker productivity or intention. Games that take the form of separate software packages are prohibited. Use of e-mails for chain letters, charitable solicitations, political campaign material, religious work, transmission of objectionable material, or any other non-business use is prohibited.

4.2.2 User IDs And Passwords

To implement the need-to-know process, JORJAR Ltd requires that each worker accessing multi-user information systems have a unique user ID and a private password. These user IDs must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each worker is personally responsible for the usage of his or her user ID and password.

4.2.3 Anonymous User IDs

Users are prohibited from logging into any JORJAR Ltd system or network anonymously, such as by making use of "guest" user IDs. When technical staff employs system commands that permit them to change active user IDs to gain certain privileges, they must have initially logged on employing user IDs that clearly indicated their identities.

4.2.4 Difficult-to-Guess Passwords

Users must choose passwords that are difficult to guess. This means that passwords must not be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used.

4.2.5 Choosing a Password

Users should choose easily-remembered passwords that are at the same time difficult for unauthorised parties to guess. Guidelines for selecting safe passwords include the following:

- Random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols should be utilised.
- Avoid using a word found in an English or foreign dictionary.
- Use the first letter of each word from a line of a song or poem;
- Choose two short words and concatenate them together with a punctuation or symbol character between the words, like for example "chair%oak"

4.2.6 Repeated Password Patterns

Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. Users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

4.2.7 Password Constraints

Passwords must be at least 8 characters long, the more characters a password has the safer it is; however it would be more difficult to remember. Passwords must be changed every 90 days or at more frequent intervals. Whenever an employee suspects that a password has been compromised, that password must immediately be changed.

4.2.8 Password Storage

Passwords must not be stored in readable form; this means that passwords must not be written down or stored on a computer in some readily decipherable form. Should a password have to be stored, it should not be left in a place where unauthorised persons might discover it.

4.2.9 Sharing Passwords

Sharing of account login information is prohibited. The only time when a password should be known by another individual is when it is first issued. These temporary passwords must be changed the first time that the authorised user accesses the system.

4.2.10 Group Login

Each individual user needs to have a unique username and password; each member of staff should have a single unique user ID and a personal password for access to JORJAR Ltd.'s computers and networks.

4.2.11 Use of Electronic mail

Employees must not play practical jokes, engage in pranks, or otherwise humorously make it look like a security incident is taking place, will take place, or has taken place when this is not true.

Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. If such messages are received by employees, they must speak directly to the sender of offensive communications. If such offensive messages do not cease, they will be reported to their manager and the Human Resources department where disciplinary action will be taken.

Before sending an e-mail, employees must verify that they are sending it to the correct contact. If it is suspected that an error has caused third party secret or confidential information to be exposed to unauthorised persons, these third parties must be immediately informed. If the third-party individuals are notified about breaches, or even seriously suspected breaches, they will be able to take protective action.

4.2.12 Employment Termination

User access should be reviewed periodically by management at least annually to ensure access levels comply with the level of access required by the individual's role.

Human Resources should inform any changes in worker duties or employment status promptly to the Information Security Department. For all terminations, the Human Resources department should also issue a notice of status change to all managers who might be responsible for a system on which the involved worker might have had access to. The terminated user's access rights should be immediately revoked.

4.3 Change Management Policy

This policy helps to minimise the risk of negative effects brought about by changes to JORJAR software, network or hardware by outlining procedures to be followed when implementing changes thus ensuring that they are implemented correctly.

The main aim of this policy is to avoid having critical errors and downtime brought about by changes in the organisation's core applications, network resources and hardware by employees and third parties.

4.3.1 Information Security Manager

The IS Manager is in charge of authorising change requests and ensuring that they have been carried out correctly.

4.3.2 The IS department

The IS department ensure that changes to JORJAR systems are correctly carried out.

4.3.3 The Website Hosting Service Provider

The webmaster ensures the correct implementation of changes to the website.

4.3.4 Software Providers

The software provider being SportingTech (<https://sportingtech.com>) is in charge of providing patches and upgrades to the software.

4.3.5 The Change Management Process

The integrity of JORJAR systems has to be maintained at all times; therefore, the procedures outlined within this document must be followed whenever any changes are carried out.

The Master licensor will be notified of any changes to software, hardware, and network configuration through an incident report (Appendix A), and any other gambling Authority will also be notified as per its jurisdiction requirements. In particular, this will include any changes to the Key technical setup and essential components, and before a new product vertical or game is added to the product portfolio. Should JORJAR plan to schedule a major change to the system, particularly any critical changes affecting the essential components or critical elements of an approved game, initial approval is sought in writing from the Master Lisensor or other relevant gambling Authority before the change goes into the planning stage. Any non-critical changes will be notified to the Master Lisensor within 30 days of the change.

Once the change is implemented in the production environment, the respective gambling Authority will be notified so that the Authority is kept updated at all times, in order to confirm that the implementation is in line with what was originally authorized.

The flowchart below highlights the change management process, which is followed for every change carried out by JORJAR as well as any third parties who are carrying out changes to JORJAR systems.

4.3.5.1 Change proposal

Whenever the need for a change is identified, a change proposal is sent in ticket, Slack or writing by e-mail to the Information Security Department, who should log and prioritise the request. The request is then forwarded to senior management for consideration.

Change Requests normally include the following information:

- The area which is in need of change
- The problem identified and why there is the need for the proposed change
- The benefits they think will be gained from implementing the change

4.3.5.2 Cost Benefit Analysis & Impact Assessment

The Cost Benefit Analysis involves identifying and listing out the potential costs of the proposed undertaking and the expected benefits.

An impact assessment is also carried out to see if the proposed change will bring about any other changes and identify any potential problems before they arise.

This exercise helps management to decide whether the change is viable or not by calculating the risk involved in carrying out this exercise. This process is the main determinant of whether the change request is accepted or not. If the change is approved, a budget is allocated to this project, and the request is forwarded to the department or third party handling this change.

4.3.5.3 Testing of Changes

Once work on the proposal has finished, testing is carried out to see if the finished product has any adverse effects on the system or network.

Irrespective of whether the change was carried out on software, hardware or network, testing on a virtual environment is carried out. This virtual environment is a subset of the live system suitable for testing with sanitised data, and is used to detect any potential issues before implementation.

User acceptance testing is also carried out (where applicable) to ensure that the changes meet the user's final needs and expectations before the change is implemented in the production environment.

The Compliance Key Function (where applicable) shall test that the changes were carried out effectively so as to ensure compliance with any applicable gambling legislation.

Testing is always documented and approved by the IS Manager. Once testing is successful and approved, then the change is implemented.

Once the changes have been made then the appropriate Incident Report will be completed and filed with to the relevant gambling Authority/ies.

4.3.5.4 Post Implementation Review

After the change is implemented, a review is carried out to see if it is what was expected. This step helps management decide whether the change brought about the desired effect and if it was successful or not.

4.3.6 Hardware Changes

Should the change have resulted in any decommissioned equipment then the relevant Change in Technical Setup is to be notified to the Master Lisensor and/or other gambling Authority.

In case of an emergency, the Compliance Key Function will be in charge of filing an Incident Report within 72 hours. In case of any changes requiring tags to be broken, a request must be sent to the Master Lisensor to reseal the equipment.

4.3.7 Changes to the website

If any changes need to be carried out on the website, the IS Manager evaluates the change request before authorising the webmaster to carry out the changes. The Compliance Key Function also reviews the updates on the website to ensure that the content complies with Master Lisensor and other relevant gambling Authorities' requirements and Regulations.

Before being released on the live website, the changes are reviewed one more time by the IS Manager.

With respect to any changes when a new game, or a new B2B platform is added, provided that the Game Vertical, RNG, Game Engine, and/or Game Provider are already approved, the Master Lisensor shall be notified within five (5) days following the addition.

4.3.8 Emergency changes

Changes of a critical nature may be required from time to time to quickly address serious issues. Emergency changes follow the same procedure highlighted above; however, these are given top priority and key individuals will be involved in order to carry out the change in the least time possible.

Emergency changes would still need to go through the approval stages.

4.4 Financial Accounting Policy

4.1 Purpose

The main purpose of these procedures is to provide the information needed for sound decision making and to ensure the timely preparation of the financial reporting required by the relevant gambling Authority.

4.2 Objective

This policy aims to satisfy the specifications set out in the applicable gambling Authority's Regulations, pertaining to the financial accounting reporting.

4.3 Responsibilities

The financial and accounting procedures are being taken care of in-house, ensuring that:

- Management Accounts and Financial information are prepared,
- Gaming Tax (Compliance Contribution) is calculated,
- Monthly liability reports are prepared and submitted on time.

Procedure

Summary of reports

Reports submitted annually:

- A copy of the interim financial statements – from the half yearly period of the financial year
- A copy of the insurance policy (if applicable)
- License Fee

Report to be submitted half-yearly:

- A copy of the Audited Financial Statements are to be submitted within one hundred and eighty (180) days from the end of the financial year

Reports submitted monthly

- Management Accounts
- Documentation with regards to Players' Funds. This submission should include:
 - A reconciling of month-end balances of all players' funds (including both the account's currency as well as its Euro equivalent),
 - Funds held in credit institutions,
 - Funds in transit,

- Statements from credit institutions and payment service providers supported to support this submission,
- Month-end player liabilities,
- Gaming System report to support this submission,
- The calculation of the Compliance Contribution and any other tax due are to be calculated, and paid are to be effected within the twentieth (20th) day of the following month including the relevant documentation used for the computation

Accounting and Reconciliation procedures

Management accounts are to be compiled least on a quarterly basis. The accountants will carry out all the necessary reconciliations to better help management when taking decisions in respect of the business.

It is important that this information is generated regularly so any decisions taken are based on data which is up to date. Such data will be useful for future planning of expenses, investments, and strategies to push the business forward.

The accountants will also have access to data generated from the back office, as well as third parties such as payment service providers.

Annual reporting

The Corporate Services provider will, within one hundred and eighty (180) days from the end of its financial year, file with the gambling Authority an audited set of financial statements prepared in accordance with the International Financial Reporting Standards (IFRS).

The Corporate Services provider shall pay an annual license fee to the gambling Authority. This is to be submitted every year and in advance.

4.5 Fraud Management Policy

See Appendix A.

4.6 Information Security Policy

The document aims to better establish management direction by laying the necessary procedures to help safeguard JORJAR Ltd confidentiality, integrity and availability of all of its business assets.

This document was written with the following considerations in mind:

- To establish safeguards to protect information resources from theft, abuse, misuse and any form of damage and establish responsibility and accountability for Information Security in the organisation.
- To create an appropriate level of awareness, knowledge and skill to allow both staff and management to minimise the occurrence and severity of Information Security incidents.

This policy should be read in conjunction with all JORJAR Ltd Policies and Procedures.

All JORJAR Ltd Policies and Procedures are subject to an annual revision where documents are updated if necessary in order to ensure that all documents are true to the organisation's current operation.

4.6.1 Information Security Manager

The Information Security Manager will be responsible for protecting and safeguarding data, maintaining the Information Security Policy and in charge of Risk Management as well as be in charge of enforcing this policy and ensure that adequate training/advice is given to new staff who should be aware of the information security best practices and procedures as outlined in this and any other relevant documents.

4.6.2 Team Effort

To be effective, there should be a team effort involving the participation and support of every employee who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the steps they must take to help protect JORJAR Ltd information and information systems.

4.6.3 Safeguarding of data

Information is a vital asset and all accesses to, uses of, and processing of, JORJAR Ltd information must be consistent with policies and standards.

JORJAR Ltd information, and information that has been entrusted to JORJAR Ltd , must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with its classification, no matter what its stage in the life cycle from origination to destruction.

4.6.4 Classification of Data

JORJAR Ltd has adopted an information classification system that categorises information into four groupings. All information under JORJAR Ltd control, whether generated internally or externally, falls into one of these categories; all workers must familiarise themselves with the definitions and the steps that must be taken to protect the information falling into each of these categories.

Public - This information has been specifically approved for public release and unauthorised disclosure of this information will not cause problems for JORJAR Ltd , its customers, or its business partners. Examples are marketing brochures and material posted to the web page. Disclosure of information to the public requires the existence of this label, the specific permission of senior management, or long-standing practice of publicly distributing this information.

Internal Use Only - This information is intended for use within JORJAR Ltd , and in some cases within affiliated organizations, such as JORJAR Ltd business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for JORJAR Ltd , its customers, or its business partners. This type of information could already be widely distributed within the company, or it could be so distributed within the organisation without advance permission from Management. Examples are the Company's telephone book and most internal electronic mail messages.

Confidential - This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for JORJAR Ltd , its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information Owner. Examples are customer transaction account information and worker performance evaluation records.

Secret - This information is the most private or otherwise sensitive, and must be monitored and controlled at all times. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause severe problems for JORJAR Ltd , its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the Senior Management. Examples are merger and acquisition plans and legal information protected by attorney-client privilege.

It should be noted that there might also be data which is maintained by JORJAR Ltd , which should not even be in readable form. This includes players passwords which should be one-way hashed using the SHA-512 or other hashing protocol, and the players' credit card detail should the company decide to start saving such information.

Default Category - If information is not marked with one of these categories, it will default into the Internal Use Only category. If information falls into the Internal Use Only category, it is not necessary to apply a sensitivity label. Information that falls into the Confidential or Secret categories is designated Sensitive.

4.6.5 Safeguarding Applications

Computers and networks should not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors approved by JORJAR Ltd. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from un-trusted sources should not be used unless it has been subjected to a rigorous testing regimen approved by the Information Security Department.

From the front-end side accessed by the player, it shall be ensured that all pages are to be running on the HTTPS secure protocol.

Virus Screening - All personal computers must have the current versions of approved virus screening software enabled. Users must not abort automatic software processes that update virus signatures and periodically scan the terminals. Virus screening software must be used to scan all software and data files coming from either third parties or other JORJAR Ltd groups. This scanning must take place before new data files are opened and before new software is executed. Workers must not bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

Virus detection - If workers suspect infection by a computer virus, they must immediately stop using the involved computer and the Information Security department. Any portable storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves, but a qualified JORJAR Ltd staff or consultants must complete this task in a manner that minimizes both data destruction and system downtime.

4.6.6 Portable Computers

Employees in the possession of a portable device; example a laptop, notebook, handheld, and other portable computers containing Confidential or Secret information must not leave these computers unattended at any time unless the information is stored in encrypted form.

Employees in possession of portable computers containing unencrypted Confidential or Secret information must not check these computers in airline luggage systems or with hotel porters; however, these computers must remain in the possession of the traveller as hand luggage.

Whenever Confidential or Secret information is written to a portable storage device, the storage media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media must be stored in a locked safe, locked furniture, or a similarly secured location.

4.6.7 Remote Printing

Printers must not be left unattended if Confidential or Secret information is being printed or soon will be printed. The persons attending the printer must be authorised to examine the information being printed.

Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorised to see the material being printed may not enter.

4.6.8 Safeguarding of Networks

Servers and workstations should include sufficient automated tools to assist the system administrator in verifying a system's security status. These Intrusion Detection tools should include mechanisms for the recording, detection, and correction of commonly-encountered security problems.

Logs containing computer or communications system security relevant events should be retained for at least three months. During this period, logs should be secured such that they cannot be modified, and such that only authorised persons can read them.

Certain information should be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information should be securely stored offline until such time as it is determined that JORJAR Ltd will not pursue legal action or otherwise use the information. The information to be immediately collected should include system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files. Records reflecting security relevant events should be periodically reviewed in a timely manner.

Users must be informed of the specific acts that constitute computer and network security violations. Users must also be informed that such violations will be logged.

Although system administrators are not required to promptly load the most recent version of operating systems, they are required to promptly apply all security patches to the operating system that have been released by knowledgeable and trusted user groups, well-known systems security authorities, or the operating system vendor. Only those systems security tools supplied by these sources or by commercial software organizations may be used on computers and networks.

Handling Network Security Information - From time to time, the Information Security Manager will designate individuals to audit compliance with this and other computer and network security policies. At the same time, every worker must promptly report any suspected network security problem, including intrusions and out-of-compliance situations, to the Information Security manager.

4.6.9 Safeguarding of Equipment

Additionally, for protection from fire, floods, earthquakes, or any forms of natural or man-made disasters, Office and Production environments should contain physical security barriers, such as biometrics and / or card-controlled entry systems.

Access to JORJAR Ltd systems should only be granted by entering unique credentials, which identifies each member of staff. The use of generic credentials is not allowed by the company.

All critical equipment should be protected and maintained by making use of devices such as an Uninterrupted Power Supply (UPS) in case of power failure and Surge protectors to avoid damage to equipment when there is a fluctuation in electricity.

Equipment should also be given situated in an appropriate air-Conditioned environment.

4.6.10 Disposal of Equipment / Media

When sensitive information is erased from a disk, tape, or other reusable data storage media, it must be followed by a repeated overwrite operation in order to obliterate the sensitive information.

Before any computer storage media is sent to a vendor for trade-in, servicing, or disposal, all JORJAR Ltd sensitive information must be destroyed or concealed according to methods approved by the Information Security Manager.

The disposal of all paper documents that contain payment information such as bank account numbers or credit card numbers, must involve shredding or other approved destruction methods.

Equipment which needs to be securely disposed of has to follow the correct procedure (refer to the Incident Response & Asset Removal Policy).

4.6.11 Enforcement

Every member of staff must comply with the information security policies found in this and related information security documents. Staff who deliberately violate this and other information security policy statements will be subject to disciplinary action up to and including termination.

4.7 Incident Response Plan

Incidents will be reported by the client by means of logging tickets into the Customer Support System. Choosing the correct priority level, will provide valuable time, to better distribute the workload and organize the queries accordingly.

Please note the following definitions:

- **Blocker** - "L1 Impact" : Means a defect that either prevents the running of either **Software as a whole**, in any of the individual Products (Sports; Casino; Retail).
 - **Prevents All or a significant number of End-users** from placing stakes on one or more Product(s),
 - **Prevents the access** of any Products or continue to play on these products;
 - **The payback percentage** on any Product is disproportionate by reference of any odds given or otherwise
 - **Prevents End-Users from registering** on the website
- **Critical** - "L2 Impact" : Means a defect that materially adversely affects the Software (**not amounting to a L1 Impact**), including for example:
 - The Software is not functioning as per the agreed specification criteria for functionality and is materially adversely **affecting a majority of the End-users** (e.g. a system slow down, payment methods not working)
 - Limited access to the Platform or any parts thereof (e.g. **majority of End-users** are not able to view balance; Unable to use fund on)
 - The ability of End-users **to place stakes on Products** is materially adversely affected.
- **Standard** - "L3 Impact" : Means a defect with **no direct financial impact**. The Software is not functioning to the reasonable satisfaction of the End-users, but the defect **is neither a L1**

Impact nor a L2 Impact and does not have Major impact on the users' experience, as

examples:

- The system does not automatically settle a bet resulting in an Open Bet
- Report not displaying data or incorrect values
- Frontend issues/bugs impacting users' experience

- **Minor - "L4 Impact"** : Means a request or an issue that does **not have any or very small**

impact on the End-User and/or the software, as examples:

- Users Personal Information change
- Correction of text appearing as string
- Defect on website bet history
- Technical Review of a Transaction / Transaction log

- **Trivial - "L5 Impact"** : Relates to cosmetic changes and requests that don't have any impact on the system or end-users; small text adjustments or corrections.