



Policies and Procedures

Version Number: V.1



Table of Contents

1. Information Security Policy.....	3
2. Incident Response Policy	20
3. User Management Policy.....	24
4. System Access Rights Policy.....	33
5. Financial Accounting Procedures	37
6. Business Continuity and Disaster Recovery	42
7. Backup Procedure	44
8. Change Management Procedure	45



1. Information Security Policy

1.1 Our Principles

Information belonging to or held by the Company, whether personal or non-personal ("Company Information") is a valuable asset.

Failure to protect these assets leads to their unauthorised access, use, disclosure and destruction. **Adequate protection** of these assets from unauthorised access, use, disclosure and destruction reduces this risk.

Just like any other valuable assets belonging to an individual, such as precious jewellery which is usually deposited in a safe deposit box for safe-keeping – Company Information needs to be adequately protected from thieves or fraudsters.

Inadequate security leads to or may potentially lead to a number of implications for the Company as well as for its customers, which include financial losses, judicial proceedings against the Company, loss of reputation and trust; temporary or permanent ban on data processing issued by the competent authorities if personal information is unlawfully disclosed or processed;

Effective Information Security is a financial investment for the Company. We deem it of utmost importance to ensure that Company Information is secured in such a way that any risk of threats and vulnerabilities is significantly reduced and any expected financial loss or damages resulting from such threats and vulnerabilities is also diminished.

Information Security requires an **evaluation of risks** by assessing the threats and vulnerabilities to the information and ensuring that the Company has the necessary procedures and controls in place to preserve this information in line with **confidentiality, integrity** and **availability**.

1.2 Security risk assessment

Risk of threats and vulnerabilities to the Company Information can never be fully eliminated. An element of risk however remote is always present.

Risks can however be significantly reduced – by carrying out an **information security risk assessment**.

The Company has: (i) evaluated the current state of its infrastructure, (ii) compiled an inventory of all its assets; and (iii) identified the processes used for accessing the Company Information held in its systems. From the information gathered, risks have been identified, quantified, prioritised and action mitigation controls have been determined and implemented



to protect against and reduce risks.



The controls covered by this Policy reduce the risks to an acceptable level for the business.

The Company monitors its risk mitigation plan periodically and performs annual security risk assessments to address any changes in the risk levels or security requirements¹.

1.3 Access controls

1.3.1 User Management

All access to Company Information, resources and services as well as physical access shall be restricted and controlled. Access to system documentation and software applications shall be restricted. Access to logs, personal data, business sensitive information and to intellectual property ("IP") shall be strictly restricted, assigned on a need-to-know basis and controlled according to risk assessments and relevant law.

All Users shall be assigned access rights based on the **need-to-know** access control principle. Access rights shall be assigned, audited, and removed through an access control process ensuring that access to Company Information, whether personal or non-personal, resources and services is allowed only on need-to-know or need-to-use basis.

Users shall only be provided with access to the company premises, information, resources, networks, network services and other services which they have been specifically authorized to use. The assessment of the level of access to grant a particular User shall be based on the following factors: risk assessments including any risks associated to: - insufficient confidentiality, integrity, and availability of information; insufficient traceability of the use of the resources; breaches of privacy; violation of immaterial rights. The role of the User and the nature of the role shall also be factored in.

Users shall be required to sign their contract of employment or for the provision of services in the case of third party staff members and sub-contractors which shall contain adequate confidentiality provisions and provisions related to data protection, prior to being provided with any access rights. In the event that the sub-contractor/third party staff member is an organization, any agreement must be signed by its legal representatives. The employees of that organization might be asked to sign a separate non-disclosure agreement and/or data controller-processor agreement prior to being granted access rights.

1.3.2 Joiners, Movers and Leavers

Access rights for new Users shall be determined and provided in accordance with our policy on "User Management" above.

Users who move cross-functionally, change duties or employment status within the Company shall be immediately removed of their old access rights, if they no longer require



the same level of access and granted new access rights based on the need-to-know principle. These changes are to be logged and retained by the MIS Department.

Users who resign or are released by the Company shall have all their physical, IT, and any other access rights terminated prior to physically exiting the Company premises. The Company will ensure that it has a process in place to ensure that the Users' accounts will be disabled on all systems where they have their accounts on the last day of their employment or on the day on which their contract terminates, whichever the case may be. Access can only be re-enabled upon approval from the Information MIS Manager.

A list of all leavers must be provided to the IT Department prior to the last day of employment/expiration of the contract. If a User's contract or employment is being terminated by the Company for HR reasons, his/her account must be disabled before or during the exit interview.

Each User shall be given an exit interview in order to collect keys, cell phones and other equipment and to sign any documents or contracts which might be required. Subject to the termination of the User's employment or contract for HR reasons, once these actions are performed, the account of the User is immediately terminated and deactivated.

1.3.3 Restricted Physical Access & Controls

Certain areas both within the Company offices and outside the main offices ("Premises") are considered more security sensitive than others, such as the server locations.

Physical access to the server location centre is limited to access on a **need-to-know** basis. Only a limited number of authorised employees and other representatives of the Company when requested or when necessary, will be granted access to the Company servers. Unaccompanied access to the equipment rooms is not allowed.

Authorisation levels and access rights to our offices and server rooms are administered and approved by our MIS Department.

Physical access to the Company's offices has been controlled by means of the following **measures**:

- Minimum entry points;
- Identification badge and access card;
- Locks on doors and cabinets.

The Company Premises will be **monitored** with security cameras all times and the footage shall be retained for a limited defined period as provided in our Retention Policy, after



which it shall be properly disposed of in accordance with this Policy² (see “Disposal”). The security cameras will cover the entire area of the premises, with the exception of the restrooms and other areas prohibited by law from being monitored. Appropriate standard operating procedures will be applied to all security camera equipment and applications to ensure effective and ethical management of the equipment as well as appropriate maintenance of the footage by authorised users. The Company will ensure that the below measures are taken in relation to the installation of the security cameras within the Premises:

-

- All security cameras will be installed in secure areas within the Company Premises;
- Easily visible signs shall be placed in all monitored areas;
- Access to the security camera equipment and footage will be restricted to authorised users;
- The footage will be processed and retained in accordance with data protection legislation and will only be accessed in the event of a security investigation.

The Company acknowledges that the security cameras may also capture and record the movements of its employees during working hours. To this effect, the Company will ensure that all employees will be adequately informed and will obtain the necessary consents from the same for the processing (capture) of their images.

The Company shall regularly monitor the security camera equipment to ensure that each security camera is still appropriate for the task as well as to effect any changes to the positioning of the same following any modifications carried out to the areas/building.

All employees and visitors authorized to access the Company Premises must display prominently at all times an identification badge and access card issued by the Company, which displays:-

- the individual’s full name;
- the employing company;
- the type of identification (employee, contractor, visitor);
- a photograph (solely in relation to employees).

Tracking and monitoring of physical access to the Premises is provided by:

- security cameras;
- the verification of visitors’ identity and entry into the premises;



- the logging of exit and entry details from the access card/identification badge;
- monitoring of network access.

All our employees are trained and fully aware:

- To report any suspicious activity to their manager;
- To escort their visitors throughout the duration of their visit;
- To courteously challenge any employee or visitor if the badge is not displayed;
- To shred all confidential documents upon completion of the task;
- To authorize and record all movement of material entering and leaving the premises;
- To forbid tail-gating;
- Not to permit photos taken in processing facilities;
- To keep their access cards/identification badges in a safe place when they are not within the Company Premises;
- To report lost or presumably stolen access cards/identification badges immediately in accordance with the Company's escalation procedure;
- Not to permit others, including other employees/colleagues to use their access card.

1.3.4 Visitor Access

Visitor access to the Company's Premises is strictly controlled.

Only designated authorised key personnel have physical access to the server room, as authorised by the MIS Department.

In order for a visitor to be granted access to any server room, they must be identified with proper official identification to ensure that they have the correct authorization. When such visitors have been allowed entry to the site, at least one employee will escort the visitor during the whole visit. In no circumstances will the visitor be allowed to be present at the data centre without supervision. All visitors are assigned a visitor card (badge/access card) to identify them at any time when inside the facility so that they can be distinguished from the data centre employees.

Visitors will have to report to the reception area of the Company's offices to gain entry. Entry to the reception area from outside is controlled by the receptionist. Entry within the offices beyond the reception area is not possible until a visitors badge is issued. Issuing and logging of



the visitor is performed with the receptionist. On leaving the company, visitors are logged out and the badges are collected.

1.3.5 Remote Access for Users

We promote teleworking within our organization. Remote access provides a similar experience to “working from the office”: once connected the User is placed on the corporate network via a virtual private network (“VPN”) connection using the approved VPN client and appropriate authentication (two-factor).

Remote access to Company Information by Users may be allowed after applying the adequate protective measures in accordance with the results from the Company’s information classification or risk assessment. Remote access of each User is approved by the MIS Department.

Remote access is also restricted to authorised members and representatives of gaming authorities when requested or when necessary.

1.3.6 Session Time-Out

All sessions shall be automatically shut down after 15 minutes of inactivity. Users must input their login details and reconnect via VPN, if connecting remotely.

1.3.7 Password Management

All Users must input a unique User ID and a password (two-factor authentication) in order to be able to access the Company’s systems.

1.3.8 Employees’ Password Management

Temporary passwords are assigned to Users upon commencement of employment. Users are advised to change this password immediately after the first login to one of their choice.

The Company raises awareness internally on the importance of **good and effective password management**, in particular it stresses the importance of the following:-

- Passwords allowing broad access to Company information systems must be different to passwords used for personal accounts;
- Blank-field passwords are not allowed by the Company and its systems are designed to automatically reject any blank field passwords.
- Passwords must contain not less than 8 characters.
- A combination of upper and lowercase and alphanumeric characters and at least one special character;



- Each password must have a lifecycle of 30 days. Upon the expiry of the 30 days, the user shall be prompted to change the password. If an account or password is suspected to have been compromised, Users shall be required to change their passwords immediately and report the matter in accordance with our Incident Response Policy;
- Inactive accounts (no activity for 3 months or over) and accounts of employees who have terminated their employment with the Company shall be disabled;
- Users should opt for passwords which are not easy to guess, or which can be easily associated with them such as nicknames, pet names, known interests, common dictionary words, birthdays.
- Passwords cannot be reused.
- Users are responsible for their passwords and must refrain from disclosing the same and any other login details to anyone including family members. Users shall also refrain from writing passwords down or store them online or on their devices.
- The User will be locked out from the system after six failed access attempts (such as inputting of wrong password). The lockout duration will last for 30 minutes or until the system administrator re-enables the User ID, whichever is the earlier.
- Passwords must be re-entered after 15 minutes of inactivity.

1.3.9 Device and Equipment Management

- Desktop, Portable Devices, Storage Media and Peripheral Equipment

The Company may provide desktop as well as mobile devices including laptops, mobile phones, tablets and storage media (such as USB pen drives, DVD/CD, etc) to employees and other Users whose role requires them (collectively “Devices”). Users are able to access internal e-mail, calendars and contacts, as well as other resources and applications available on the internal network from mobile phones, tablets and laptops, as if they are accessing these from their desktops.

Each of these hardware Devices, including peripheral equipment such as fax machines, printers and photocopiers, has the ability to create, receive, store, access or share Company Information.

Hardware forming part of the key technical setup will only be located in the premises which adheres to a high level of information security.



Security measures for peripheral equipment include: -

- Photocopiers, printers and fax machines that store or transmit confidential or sensitive information shall be placed in secure locations and monitored.
- All documents containing confidential or sensitive information shall immediately be cleared from printers, copiers and fax machines.

Portable Devices present a special risk purely due to their mobility and as a result are vulnerable to theft (consequently to data theft) and loss. Therefore, the Company recognises the importance and necessity of applying extra security measures to protect the Company Information stored within those Devices.

Users who are granted access to the Company's network or information systems shall adequately secure their Devices from unauthorized access.

Best practice security measures implemented by the Company include the following safeguards: -

- Devices should be locked when unattended;
- A password system must be used, or PIN code must be activated on the Device to protect the contents of the same;
- Devices must be protected at all times from heat, cold, water, smoke, dust, physical damage and magnetic interference;
- Devices should not be used in public places to avoid situations where passers-by might have visibility of the contents of the display;
- USB Mass Storage Devices must be removed from the Device when not in use, stored securely and returned to the MIS Department when no longer required;
- The Company should be informed immediately if the Device is misplaced, stolen or presumed stolen. This would enable the Company to take the necessary immediate security measures to protect the Company Information stored on the Device, including remote Data Wipe-Out³.

The Company provides local and network storage within the organization to easily manage and store files, thus reducing the use of removable storage Devices for most day-to-day tasks.



³ See “Remote Data Wipe”

Given the large amount of information which removable storage media Devices can store, the Company has defined **additional controls** to minimise risks.

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 MIS Department.
- Data can only be stored in a Company provided storage device;
- We could not use USB storage device.

The Company does not encourage the use of online file hosting services to reduce risks. Users shall be unable to download such applications onto the company-owned Devices as this functionality will be disabled.

1.3.10 Usage of Personal Devices

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 must be requested from the MIS Department to connect their personal mobile devices to the company servers.

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 measures⁴;

1.3.11 Remote Data Wipe

Although there are circumstances where Users can access Company Information through their personal Devices, any Company Information created, received or stored within that personal Device remains the property of the Company at all times. To ensure adequate protection of Company Information, the Company will require the User to acknowledge this Policy on use of personal devices as well as specifically consent to the fact that once the User no longer requires access to Company Information from the personal Device, all Company Information, namely emails (corporate email account) and work calendar will be remotely wiped-out, before access is provided. The User shall also acknowledge that whilst the Company shall use its best efforts to ensure that only Company Information will be erased from the personal Device, it cannot exclude the possibility of erasing personal data



⁴ See: "Desktop, Portable Devices, Storage Media and Peripheral Equipment"

stored within the Device, apart from Company Information. The User shall be fully aware that this might happen and is responsible to ensure that s/he regularly backs-up his/her personal content stored on the Device. The User shall also acknowledge that s/he will not hold the Company responsible, if this happens.

If the Device whether personal or Company-owned, is stolen, misplaced or presumed stolen, the user is obliged to inform the Company immediately and without undue delay. The Company shall immediately initiate a "Lock" and Remote Data Wipe of the Device.

1.1 Disposal

1.1.1 Disposal of Media and Equipment

The disposal of electronic records stored on media, computer equipment, and computer software can create information security risks. These risks are related to the potential unauthorized disclosure of Company Information, violations of software license agreements, and unauthorized disclosure of intellectual property that could be stored on storage media, computer equipment, and computer software.

This Policy governs the requirements of secure disposal of media containing Company Information, as well as the secure disposal of Company Information stored on other equipment, by establishing a process which ensures the secure removal of sensitive data or protected information from storage media or from the equipment, prior to disposal.

This Policy covers all fixed and removable storage devices and all equipment such as Devices owned by the Company. This includes but is not limited to: magnetic media (including fixed disks, magnetic tape, floppy, and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), PDAs, laptops, desktops. Any storage devices or Devices currently available, or which may become available in the future due to new technology, are also covered by this Policy.

- The Company shall assign the responsibility of disposal to a member of its staff with a suitable level of authority who shall authorize the disposal and shall be responsible to maintain a full inventory of all equipment including media which has been marked for disposal;
- The Company will opt for the appropriate disposal methods upon taking into consideration the security vulnerabilities associated with each method;



- All electronic Devices and media equipment, including storage media in personal computers and other hardware containing Company Information, must be degaussed (demagnetised) prior to disposal so that the data will not be



retrieved and reused. The sanitisation methods used will depend on the type of media and the intended disposal of the media.

- Non-functioning and/or non-writable media containing Company Information must be physically destroyed if degaussing or other sanitisation is determined to be inadequate.
- Disposal of media requires authorisation and tracking by MIS Manager.
- Where possible, destruction will be performed on-site.
- Damaged media and drives cannot be sent for repair and must be physically destroyed.
- All methods of media disposal shall be in compliance with information security best practices.

The Company reserves the right to either internally re-deploy Devices especially desktops, laptops and mobile phones or donate/sell them to third parties outside the organisation, instead of destroying them. The Company shall however make sure that all Company Information including any software and any other residual data are properly deleted from the Devices prior to the re-deployment, donation or sale.

1.2 Safeguarding of Applications

1.2.1 Application Security

- Privacy and Security are integral components of software development life- cycle. All applications developed by the Company must have documented security analysis included in the specification and design documentation, following a security risk assessment. A privacy impact assessment must also be carried out in the early stages of development to cater for any privacy risks prior to the deployment of the application (“**Privacy By Design**”).
- All applications must be developed according to security best practices and international standards (such as ISO 27001 “Information Security Management”; ISO 27002 “Information technology- Security techniques-Code of Practice for Information Security Controls” and any other international standards which may be applicable).
- Any modification to core functionality must be peer reviewed.
- Any application modifications with security and/or privacy implications must be



signed-off by the MIS Manager before a release. Notwithstanding the security

and privacy impact assessments, all applications must still be tested for common security and privacy weaknesses before deployment and no application should be released containing known security and/or privacy vulnerabilities.

- All developers must be familiar with common application security and privacy weaknesses.
- No test or debugging functionality can be present in final product builds.
- Management interfaces must only be reachable through the internal network and never exposed publicly, even if restricted to a set of addresses or if protected by a password.
- Application documentation must include Security controls and Security test plans.
- Each application is integrated with static source code analysis nightly build.
- All applications must be classified in order of required security level.
- Critical applications are subject to an annual audit plan.
- Third-party components in our developed applications fall inside scope.

1.3 Safeguarding of equipment

1. We installed the TrustView for record and monitor personal computer

TrustView): VDP (Virtual Disk Protection) utilizes proprietary technology in virtual disk isolation to provide a solution to the need of enterprises in protecting various kinds of internal documents, especially R&D design files with unique format or program files which could be damaged. Furthermore, it can protect existing web application system without the need for system integration. The special thing is that while protecting the company's important data, it can also proactively defend against the attacks of ransomware at the same time!

2. The only way we could connect to company's computer through VDI and there will be record every actions.

Virtual Desktop Infrastructure, VDI



The Company has the right to monitor any and all aspects of its phone and computer systems for security purposes as well as monitor and/or access communication logs, including without limitation those related to phone (company-owned), corporate email accounts or internet communications upon reasonable grounds of suspicion of any unlawful activity by any User or upon any threat, whether immediate or otherwise to the security of the Company Information. The Company shall however make sure that all Users are informed of the Company's policy on monitoring of communications.

1.4 Network Protection

1.4.1 Network Hardware

1. We turn on the firewall for protected network access
2. Mac filtering limits the allowed associations to the Wireless Access Point to only approved network cards.

Network Systems

The Company's network systems are protected by firewalls, passwords and authentication requirements, VPNs and encryption.

1.4.2 Emails

The Company's email system shall not be used for unlawful purposes, namely it shall not be used for the creation or distribution of any illegal, disruptive or offensive messages, including spam. Subject to the above provision on the right by the Company to monitor aspects of its systems, the privacy of the content of emails will be respected. There might be exceptional circumstances (such as upon reasonable grounds of suspicion of any unlawful activity by any User or upon any threat, whether immediate or otherwise to the security of the Company Information) where the Company may require access to the Users' corporate emails and content for investigation purposes.

The Company acknowledges that Users might use a reasonable amount of the Company's resources for personal emails (non-work related emails) and this is deemed acceptable by the Company. Personal emails shall be saved in a separate folder from work related email.

Users must check all information they communicate to others via email to ensure that Company Information is not transmitted unintentionally and should refrain from sending internal emails to external parties.

Users should report any suspicious emails (such as suspicion that an email contains a virus or if an email has been received from an unknown source) to the MIS Department.



1.5 Antivirus/Antimalware Protection and other Perimeter Controls to Minimise Threat of Intrusion

The Company shall implement the necessary perimeter network controls to prevent or minimise the risk of penetration of the Company's network from the outside. Some of the measures taken by the Company include: antivirus applications, firewalls, VPNs and encryption. The Company shall also use intrusion detection and intrusion prevention systems.

antivirus: Symantec

VPNs: SSLVPN、VDI

Windows Firewall

1.5.1 Antivirus/Antimalware solutions

The Company shall install the necessary antivirus/antimalware protection within its infrastructure to protect critical desktop and server operating systems against viruses, spyware, rootkits and other security threats. It also ensures that the firewall is active and working efficiently to protect against network layer threats. Incoming and outgoing emails shall be scanned for viruses and any email attachments shall be scanned for spyware or adware applications. The Company shall ensure that the antivirus/antimalware protection will run continuously and will automatically update virus definitions and software as well as generate audit logs.

Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, bacteria, worm, Trojan horse, or the like).

Suspected viruses should be reported immediately to the MIS Department. The Company shall immediately inform the relevant authorities as soon as malicious code or suspicious codes are discovered in the system. The Company shall also take the necessary immediate steps to ensure that the malicious code does not affect the Company's systems and the Company Information stored therein.

1.5.2 Encryption and Authentication

The Company understands the importance of ensuring effective system security by implementing the necessary and adequate security controls and preventing unauthorised access to, use and disclosure of Company Information. An important measure is the



encryption of information.



The exchange of confidential or sensitive information, as classified in our Information Classification policy via email or otherwise, shall be encrypted.

TLS client certificate

We use encrypting/decrypting with TLS

The Company acknowledges that encryption alone is not sufficient. Whilst encryption ensures that the information remains confidential, it cannot authenticate the information, and this might lead to the risk of repudiation. The Company shall implement authentication measures such as digital signatures to minimise this risk

We do use Digital Signature

1.6 Information Asset Management

1.6.1 Clear Desk/Screen Policy

The Company's clear desk/screen policy complements the best practice security measures mentioned above⁵.

1.6.2 Clear Desk Policy

- Desks and workstations should be clear of all confidential and sensitive information, when the Users are away from their desk or office. Paper and storage media should be stored in lockable cabinets or any other lockable storage when not in use, especially outside working hours;
- Where lockable storage is not available, office doors must be locked if left unattended. At the end of each working day all Company Information should be removed from the workstation/desk and stored in a locked area;
- Confidential and sensitive information, when printed, should be cleared from printers immediately. Where possible printers with a 'locked job' facility should be used;
- Any visit, appointment or message books should be stored in a locked area when not in use;
- The reception desk should be kept as clear as possible at all times.

1.6.3 Clear Screen Policy

- Desktop and laptops must not be left logged on when unattended and must be password protected. The Windows security lock should be set to activate when there



is no activity for a short pre-determined period of time and should be password protected for reactivation;

- Computer screens must be strategically positioned, away from the view of unauthorized persons.

1.7 *Retention*

Retention of Company Information by the Company can be required from a legal, regulatory or business perspective. Company Information shall be retained in accordance with the Company Information Retention Policy.

Company Information shall not be retained for a period longer than necessary, unless the Company has a specific purpose to retain certain documents for a longer period. Reasons for longer retention can be found in the Retention Policy.

1.8 *Backup*

- Server systems must be regularly backed-up using a standard backup methodology. Backup media must regularly be transferred and stored securely on or off-site.
- Sensitive and confidential Company Information must be encrypted when backed up and be capable of authorised decryption for at least as long as required for legal or regulatory compliance.
- Backup systems must be periodically tested to ensure that the procedure works as expected.
- Backup media must be archived for the retention period established in the Retention Policy.

1.9 *Information Classification*

Company Information has varying degrees of sensitivity and criticality. The higher the value of the Company Information and the higher the sensitivity, the greater the security required. Company Information must first be valued. Once a value has been given, a classification can be established and a corresponding security level can be identified and implemented.

In order to determine the asset value, the following factors shall be taken into consideration:

- the level of sensitivity and confidentiality of the information; the associated



business impact, the potential financial implications and the business needs for sharing or restricting information.

The Company has defined the following information classifications:

- Confidential;
- Sensitive;
- Public

Confidential: Company Information classified as Confidential must be highly secured and remain private. If disclosed, Confidential Company Information would significantly impact the business.

Sensitive: Company Information marked as Sensitive should be adequately secured. Sensitive information can be shared internally but not externally.

Public: Company Information which can be shared externally.



Incident Response Policy

2.1 About

The purpose of this computer security incident response guide is to provide general guidance to FaDa Ltd.Ltd users – both technical and managerial to:

- Enable quick and efficient recovery from security incidents;
- Respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident;
- Prevent or minimize disruption of critical computing services;
- Minimize loss or theft of sensitive or mission critical information.

The challenge of incident response is to be able to bring FaDa Ltd.Ltd users with divergent skills together quickly and effectively in a crisis situation. To prepare for this challenge, FaDa Ltd.Ltd has developed specific security policies, procedures and guidelines. This document provides a general overview of the preparations FaDa Ltd.Ltd has made to respond to computer security incidents and some specific help for system users when they first become aware of an incident.

2.2 Threat Environment

Although computer security incidents may take many forms and involve many devious means, there are certain types of attacks which occur more frequently than others. Knowing what these types of attacks are and how FaDa Ltd.Ltd counters them will help the users be best prepared to report and react.

2.3 Types of Threats

[include type of Threats]

2.4 Priority and Urgency

When an incident occurs, members of the Incident Response Team must effectively identify the response Level of Effort ('LoE') for the given type of incident. The following are the Incident Priorities and Urgency classifications:

- Low
- Medium
- High
- Severe
- Catastrophic



2.5 Incident Response Team (IRT)

2.5.1 Responsibilities

The IRT is a vital part of the organisation and is responsible for handling the incidents that may occur. The IRT is responsible for taking immediate action on the incident and follow the plan defined under incident management. The team is also responsible of making sure that the set procedures are followed and improve the Incident Response Policy as well as keep it updated to the procedures and the set organisation of FaDa Ltd.

Each member of the IRT shall also make sure to be available for contact at all hours and for the times not being able to be in contact, provide a backup solution.

2.5.2 Roles and Members

Primary coordinator and point of contact:

- Yintsai Huang, Director,

Incident Response Team:

- Han-Yu Liao, CTO,

2.6 Incident Management

FaDa Ltd.Ltd defines six stages of response when servicing a computer security incident:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Follow-up

Knowing about each stage facilitates responding more methodically and efficiently, and helps key users understand the process of responding so that they can deal with unexpected aspects of incidents they face. The following paragraph defines the six stages of response:

Preparation

FaDa Ltd.Ltd considers being prepared to respond before an incident occurs to be one of the



most critical facets of incident handling. This advance preparation avoids disorganised and confused response to incidents. FaDa Ltd.Ltd's preparation also limits the potential for damage by ensuring that response plans are known to all users, making coordination easier as well as securing the right course of action is undertaken.

Identification



FaDa Ltd.Ltd's approach to the Identification Stage involves:

- Validating the incident;
- If an incident occurred, identify its nature;
- Identifying and protecting the evidence;
- Logging and reporting the event or incident.

When a user notices a suspicious anomaly in data, a system, or the network, he or she begins the identification process below.

1. Customer service report issues to platform team.
2. The platform team will check issue and solved it.
3. Platform team will make records and notify the Customer service when issues was solved

Containment

FaDa Ltd.Ltd's immediate objective for the Containment Stage is to limit the scope and magnitude of an incident as quickly as possible, rather than to allow the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator.

The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. The CSO and System Owner will work within appropriate investigative organisation(s) to determine if sensitive data should be left on the system or copied to media and taken off-line. Similarly, a decision may be made to move critical computing services to another system on another network where there is considerably less chance of interruption.

Steps to be made:

1. We make limit access permissions for every role.
2. Our system has installed TrustView to monitoring operation
3. We limit the USB device so everyone could not copy files.

Eradication

The next priority, after containing the damage from a computer security incident, is to remove the cause of the incident. In the case of a virus incident, FaDa Ltd.Ltd will remove the virus from all systems and media (e.g. USB pen drives, backup media) by using one or more proven commercial virus eradication applications. FaDa Ltd.Ltd recognizes that many intrusions leave benign or malignant artefacts that can be hard to locate. Therefore, FaDa Ltd.Ltd will concentrate on the eradication of:



- Malignant artefacts (e.g. Trojan horses)
- Benign artefacts, only if they present a serious enough risk to justify the cost.

Steps to be made:

Antivirus Software find the risk file that will be remove files

MIS team will help developers clean the virus or format the disk.

Recovery

FaDa Ltd.Ltd defines recovery as restoring a system to its normal mission status.

Steps to be made:

1. MIS team will format the computer
2. We'll restore important file from backup file zone
3. Team will install software what they need
4. Re-scan computer check no virus.

Follow-up

FaDa Ltd.Ltd also realises that following up on an incident after Recovery helps to improve incident handling procedures.

Steps to be made:

1. Do not open unknown mail
2. Do not use personal device like USB mobile device etc..*

An incident report shall be submitted by the Key person responsible for the adherence to applicable legislation relating to compliance, no later than 72 hours following the incident, , in the event as a result of the incident there was downtime to the system and operations of FaDa Ltd

2.7 Contact Information for IRT Team Members

Name: Yintsai Huang, Director, FaDa Ltd Email:
andyhuang@igs.com.tw

Name: Han-Yu Liao, CTO, FaDa Ltd Email:
rainliao@igs.com.tw



3. User Management Policy

3.1 Email Usage

Email communication is one of the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across the internal network and globally via the public Internet. Conducting business via email has its risks. Emails can be insecure, particularly when transmitted outside the internal network and can be intercepted and read in transit, potentially changed and sent to the intended recipient, without the latter being aware of any alteration. It is vital therefore that the Company takes all the necessary measures to protect emails from unauthorized access and ensure that emails have not been modified or tampered with in any manner by unauthorized parties whilst making sure that the mail servers remain available for business purposes at all times.

Best practice security measures implemented by the Company, include the following safeguards on acceptable email usage: -

- All emails must be encrypted. No confidential/sensitive information can be transmitted particularly over the internet, unless it is first encrypted by an encryption system approved by Information Security Department;
- Users cannot create, send, forward or store emails with messages or attachments that might be illegal or considered offensive, sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive or any other illegal, unethical or unauthorized purpose.
- Users must refrain from committing or binding the Company towards a third party, in any manner whatsoever, including through purchase or sales contracts, job offers or price quotations, unless authorisation in writing from senior management has been obtained.
- No emails can be sent without the standard corporate email disclaimer, which is automatically appended to emails sent externally outside the organisation. Users must not interfere with or remove this disclaimer;



- Limited personal use of the corporate email systems is permitted at the discretion of the management provided always that it is incidental and occasional, and does not interfere with business. There are no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.
- Emails cannot be used in ways that could be interpreted as representing or being official public statements on behalf of the Company, unless the User is explicitly authorized by senior management to make such statements;
- Users cannot send emails or other messages from anyone else's account or in their name (including the use of false 'From:' addresses). Upon obtaining the necessary authorisation from the manager, a secretary may send emails on the manager's behalf but must always include the following wording "for and on behalf of" the manager (manager's name) beneath his or her name;

All Users must:

- check all information they communicate to others via email to ensure that Company Information is not transmitted unintentionally and should refrain from sending internal emails to external parties.
- not disclose potentially sensitive information in "out of office" messages, unnecessarily.
- report any suspicious emails to the Information Security department. Emails on the corporate IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the Company cannot guarantee however that this process is 100% effective (e.g. compressed and encrypted attachments may not be fully scanned).
- intercept, divert, modify, delete, save or disclose emails to unauthorized parties, except when specifically authorised by management or where necessary for IT system administration purposes.
- External/third---party email services (commonly known as "webmail") should not be used for business purposes.

Subject to the provisions of the Information Security Policy, the Company has the right to



monitor as well as access any and all aspects of corporate email accounts or internet communications upon reasonable grounds of suspicion of any unlawful activity by any User

1. System Access Rights Policy

1.1 About

Access control Policy lays down rules and procedures for the allocation of the rights and authorisation for accessing the data, applications and systems, and specifies the responsibilities in their implementation. The rules and procedures allow for the control of access to the information assets of the Company and reduce the possibility of unauthorised access, which may result in disclosure, loss or corruption of data.

Terms of accesses must comply with safety requirements, while enabling smooth functioning of business services at the same time. The establishment of rules is based on the categorisation of information, the applicable legislation and the contractual obligations which relate to the protection of access to information and services.

Failure to comply with the policy by the employees constitutes professional misconduct. In case of violation, the employee shall be liable and a disciplinary action might be taken against him in accordance with the applicable labour legislation.

1.2 Access rights

All system accesses are logged and these logs are available for possible audit. They will be reviewed periodically by the Pei-Hua Chen, Senior Director

System access is given only on a need-to-know basis.

In a case that a third party (other than suppliers with access) needs to access the System, they need permission from Han-Yu Liao, Senior Director and in case of physical access also the key person responsible for the network and information security. This permission will be limited to certain time frame.

Access to key systems and networks is controlled physically and logically. This means that unauthorized personnel will not have access to those areas.

1.3 Procedure detailing the assignment of access rights

Each Manager has by default permission to initiate system authorization requests for their personnel if they themselves have system access. Every request for this access must be



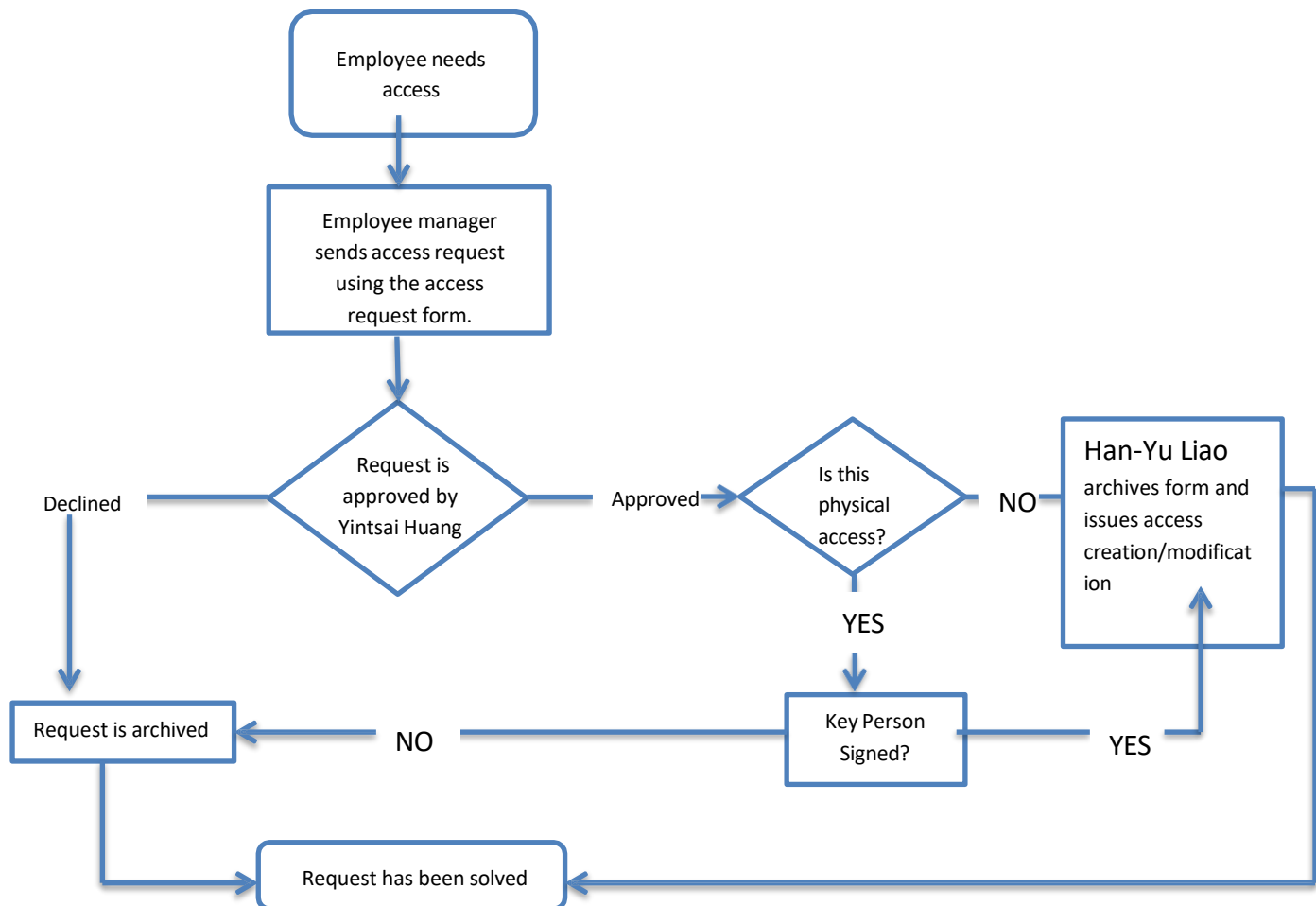
validated by Yintsai Huang, CEO.

These authorisation requests will be handled by sending appropriate form via email and emails with requests/approvals will be cc'ed to a separate account, so it will be possible to review all history.



If the request is approved, the approving authority will create an account on a corresponding part of the System.

Procedure for access is detailed below.





1.4 System access rights level per job designation

FaDa Ltd.Ltd addresses system access rights in the following ways:

Job Description	Full Access	Read Only Access	No Access
CEO	O	X	X
CTO	O	X	X
CFO	X	O	X
Systems Administrator	O	X	X
Compliance and Legal	X	X	O
CMO	X	X	O
DPO	X	X	O
Senior Developer	X	X	O
Junior Developer	X	X	O
Support	X	X	O
Third Party	X	X	O

1.1 Physical access rights

The purpose of having a physical access policy is to ensure that no unauthorized individual can be given access to the sites that are used for production. The limited access to the site will eliminate the risk of malicious actions being taken on the physical servers, and also allow traceability if an error occurs.

Job Description	Access with Supervision	No Access
CEO	O	X
CTO	O	X
CFO	X	O
Compliance and Legal	X	O
Systems Administrator	O	X
CMO	X	O
DPO	X	O
Senior Developer	X	O
Junior Developer	X	O
Support	X	O
Third party	X	O

1.2 Remote access to the system



CEO	O	X	X
CTO	O	X	X
CFO	X	X	O
Compliance and Legal	X	X	O
Systems Administrator	O	X	X
Senior Developer	O	X	X
Junior Developer	O	X	X
Support	X	X	O
DPO	X	X	O
Third Party	X	X	O
CMO	X	X	O

1.3 Regulations for visitors

Only designated Key-personnel has physical access to the data centres hosting the production environment. The designated personnel are listed as “authorized” at the data centre co-location hosting partner. The list is divided in two levels of access:

Physical: These individuals have the authorization to enter the data centre.

Designated: These individuals have the authorization to enter the data centre and also change the list of personnel who are authorized physical access. All changes must be approved by the Key Person responsible for the network and information security of the licensee (?). Designated individuals are:

- Han-Yu Liao, Senior Director.

In order for a visitor to be granted access to the data centre, they must be identified with proper official identification to ensure that he has the correct authorization. When such visitors have been allowed entry to the site, at least one employee from the co-location site will escort the visitor during the whole visit. Under no circumstances will the visitor be allowed to be present at the data centre without supervision. All visitors are assigned a visitor card (badge) to identify them at any time when inside the facility so that they can be distinguished from the data centre employees.

All visits that have followed the proper process shall be logged. The logging will record the names of the persons that have visited the data centre and the time at which they visited. The logs must be retained for at least 3 months in time.



2. Business Continuity and Disaster Recovery

2.1 Keep business recovery data and information in safe

The following should be backed up in the safe box at FaDa Ltd.Ltd:

The following should be backed up in on another data centre: Google storage

2.2 Common Disruptive Events

2.2.1 Data Loss

Data is lost due to transmission or storage. This can be due to example:

- Accidentally deletion
- Malware or virus
- Hard-drive/storage breakdown
- Power failure
- Theft of servers
- Fire

A damage analysis and start of data recovery should take place immediately within 1 hours. Backups and other sources (Payment providers, game providers) are to be used in the recovery of data. All data should be recovered within 1 hours or a damage report should be sent to the CEO.

2.2.2 Datacentre location loss

A datacentre may be lost during a short or long period of time.

To recover from a datacentre loss, the traffic should be redirected to another datacentre location within 1 hours. Within 1 hours, either the lost datacentre should be restored or replaced with a new datacentre location.

A damage report should be sent to the CEO.

2.2.3 Network loss

Due to some issues with the network to the datacentres or other connectivity, the FaDa Ltd.Ltd services might be down. This can be due to:

- Network connectivity to FaDa Ltd.Ltd
- Issues at the DNS server
- DDOS attack
- Error with network equipment at our datacentre location.



Any connectivity issues have attention within 1 hours. Traffic might take other routes and/or DDOS attack protection is turned on.

2.2.4 Staff loss

Loss of staff that have knowledge is one critical event. FaDa Ltd.Ltd should always try to have staff with redundant knowledge. Within the same day, the process to find a replacement should be started and the goal is to have new staff within 3 months. Consultants should be used to temporary fill in the knowledge gap.

2.2.5 Supplier loss

Loss of a supplier (for example bankruptcy) could have a critical impact to the services for FaDa Ltd. The process of replacing the supplier should start immediately.

2.3 Business Continuity Plan

The following steps are the most important:

FaDa Ltd.Ltd

The time required to resume normal operations following the occurrence of each identified disruptive event shall be:

1. Recovery data from backup DB (3hr)
2. Testing and Check the data is correctly (1hr)
3. Notice customer service team and urn on the entrance (1hr).

The following escalation procedure shall be implemented for each identified threat:

_ FaDa Ltd.Ltd

1. Upgrade every API from http to https HTTPS
2. Update and confirm the white IP list for restricted unknown IP access

2.4 Contact Persons

LU-HONG YU

2.5 Test the Plan

The CTO is responsible to test the plan once a year (as minimum). The CTO should initiate a test-incident to test the current plan. It is up to the CTO to decide what kind of incident to



test. A lesson learned session should take place after this test.

2.6 Alternate Sites

In an event of alternate sites, we are able to restore data and business continuity hosted on another cloud in our Belgium Data Centre - *ta-tadagaming.com*

3. Backup Procedure

We use Subversion for version control and through 7-ZIP compress the source code folder then backup to other disk (on cloud)

The System team ensures that all backups are completed successfully and reviews the backup process on all servers daily. Logs are maintained to verify the amount of data backed-up and the unsuccessful backup occurrences. In addition, a monitoring system creates reports and raises alerts in case of backup failure.

3.1 Backup Content

The content of data backed-up varies from server-to-server.

1. (everyday) Database and stored procedure
2. (1month) Source code of platform

3.2 Backup Types

Backup of non-critical servers will occur every day after regular business hours.

Full back-up:

*We backup the import data on database everyday morning (am 4:00 UTC+ 8)

*The import and data include (user coin、 user data 、 game setting 、 game-log)

3.3 Offsite Storage

Backup needs to be copied to offsite datacentre in Belgium

Restore Testing

Twice a week the restore procedure has to run to ensure backups are restorable. This will



happen in lab or development environments, using automated scripts.

Success criteria for the test – full data consistency after restore.



Change Management is a systematic approach to dealing with change, both from the perspective of an organisation and on the individual level.

3.4 Procedure

A change within FaDa Ltd.Ltd must follow the following change control procedure. A change can be a code change, or a network change, change of any system component, a firewall, patch or any other change that affects the FaDa Ltd.Ltd's environment.

The change management procedure has the following steps:

- Preparation of Change
- Call for a Change Control Board ('CCB') meeting.

If the change is approved by the CCB:

- Sought of approval of the relevant authorities where necessary;
- Deployment of the change;
- Fill in the necessary forms such as Incident Report
- A CCB approves every change that should be deployed to the Company's environment.

The chairman of the CCB is the CEO. For the decision, the following should be in place:

- What does the change contain;
- What is the impact;
- If the change affects the environment in such way that the Authority should be informed and/or part of the Risk Assessment;
- If the change needs approval by the Authority before deployment;
- Test report, including security tests;
- How to back-out.

The CCB's approval should be documented

3.5 Tools in Use

We use the following systems to support our Change Management process:

