

DMG SOLUTIONS

B.V:

InfoSec Policy

Version:	v1.2
Date of version:	3 rd February 2025
Created by:	Laurence Alexander
Approved by:	Board of Directors
Confidentiality level:	Sensitive

DMG Solutions B.V (The “Company”)

1. Information Security and Access 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.

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 and Access

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 Personnel 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

¹

the event that the sub-contractor/third party Personnel member is an organization, any agreement must be signed by its legal representatives. The Personnels of that organisation might be asked to sign a separate non-disclosure agreement and/or data controller-processor agreement prior to being granted access rights.

The company will utilise four different profiles for system access control. These profiles are outlined below:

Role	Access rights
Administrator	Administrators have full access to all systems and resources, including the ability to install applications, configure settings, and create user accounts.
Manager	Managers have access to the same systems and resources as administrators but are limited in their ability to install applications and configure settings.
User	Users have access to the same systems and resources as managers but are limited to basic operations such as reading instead of editing documents or exporting
Guest	Guests are provided access to the same systems and resources as users but are limited in the amount of time they can access the system and cannot install applications or configure settings.

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 the System Admin or CTO.

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

	Administrator	Manager	User	Guest
CEO	x			
CTO	x			
CFO		x		
Systems Administrator	x			
Compliance and Legal		x		
CMO		x		
DPO		x		

Senior Developer		x		
Junior Developer			x	
Customer Support			x	
Payments Agent			x	
Third Party				x

Users are required to adhere to measures as part of appropriate security for the control system:

1. All users must authenticate their identity with a username and password before gaining access to the system.
2. All users must have a unique username and password to access the system.
3. All users must keep their passwords confidential and change them regularly.
4. All users must be assigned a system access profile that corresponds to their job role and responsibilities.
5. Access privileges must be reviewed periodically and adjusted as needed.

Enforcement action can be taken against Personnel in breach of this policy and the following measures are set out:

1. Users who violate this policy may be subject to disciplinary action, including but not limited to suspension of access privileges, termination of employment, and legal action.
2. The company reserves the right to monitor user activity and enforce this policy at any time.
3. The company reserves the right to modify this policy at any time and will notify users of any changes.

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.

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.

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.

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 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.

All Personnel 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 (Personnel, contractor, visitor);
- a photograph (solely in relation to Personnels).

All our Personnel 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 Personnel 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 Personnels 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 CTO.

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 Session Time-Out

All sessions on the control system shall be automatically shut down after 30 minutes of inactivity. Users must input their login details and reconnect.

1.3.6 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 control systems.

1.3.7 Personnels 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.
- A combination of upper and lowercase and alphanumeric characters and at least one special character;
- 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.
- Passwords must be re-entered after 30 minutes of inactivity.

1.3.8 Device and Equipment Management

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 Personnels 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.

Users who are granted access to the Company’s network or information systems shall adequately secure their Devices from unauthorized access. Users, including managers and key persons will be given unique hardware devices, not shared with any other member of Personnel or individual.

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;

1.3.9 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.

1.3.10 Network Systems

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

1.3.11 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. 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 CTO.

1.3.12 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 CTO.

1.3.13 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 using cryptographic controls.

1.3.14 Clear Desk/Screen Policy

The Company's clear desk/screen policy complements the best practice security measures mentioned above².

1.3.15 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;

1.3.16 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.

² As listed under "Device and Equipment Management"

a. Retention

Retention of Company Information by the Company can be required from a legal, regulatory or business perspective. Company Information shall be retained for a minimum period of six (6) years.

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.

b. 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 of at least six (6) years.

c. 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.

1.4 Register of Assets

All assets are clearly identified, and an inventory of all important assets drawn up and maintained. Assets include policies, software, hardware, human resources etc.

The Company has established and will maintain registers of:

- a. Contracts and agreements;
- b. Financial accounts;
- c. URLs associated with relevant activity;
- d. Payment gateway providers;
- e. Associates;
- f. Gaming equipment;

- g. Games;
- h. Events;
- i. Excluded customers;
- j. Customers;
- k. Customer bet limits; and
- l. Assets

The above-mentioned registers shall be brought up-to-date at the end of each calendar month. When a relationship is ceased which was previously entered into a register, a cessation date shall be recorded and reason for brevity.

1.5 Segregation of duties

On a basic level, segregation of duties reduces the risk of fraud due to the fact that no single person can access and control all aspects of a system. This means that if an individual attempts to commit fraud, they will be unable to do so without the cooperation of another person.

On a more sophisticated level, segregation of duties increases the security of the Company by ensuring that no single person has control over all facets of a system. This means that if one person is compromised, the entire system is not put at risk. Additionally, it helps to ensure that different functions are completed correctly, as different individuals are responsible for different parts of the system.

It is important to ensure that all individuals within the Company are aware of the importance of segregation of duties, as well as the roles and responsibilities that come along with it. This is the only way to ensure that the system is secure and that it is not vulnerable to malicious activities.