# BMSG Information Technology Cyber Security Policy

## SECURITY

Cyber security is today at the heart of all businesses. Similarly, cyber security is at the heart of all individuals and families. In having the ability to communicate and interact by sophisticated telecommunications we (and BMSG) and you, our employees, and all stakeholders share a commitment and responsibility to delineate private information and actions from those of any business relationship.

BMSG like most companies today must identify and mitigate against an ever-increasing number of threats to its business model, IP, know-how, and eventually its continuity, ethics and ethos.

In creating a series of barriers, systems, protocols, and policies we hope to generate a team ethos that encompasses our values that face both internally and externally.

It is critical not only to BMSG continuity, but also each of our stakeholders. This is especially relevant to our personnel, that they see we share an abundantly transparent commitment to the protection of PPPI. Each day of activity, regardless of location, need to have sufficient safety and security measures that are both environmentally sound and maintain the highest possible level of protection.

Our QMS and policies support a commitment to integrating common principles within our team, and with all interactions with our stakeholders. Our impartiality and social responsibility are also implemented across our safety and security policies which are re-emphasized by this cyber security policy.

As part of our Safety and Security policies set across our QMS, BMSG offers this ITCSP as a supportive Cyber Security Policy overview regarding our operations and expectations for staff and stakeholders. Considering the extent to which we interact with and depend upon IT, the WWW and PPPI, this policy serves several purposes. The main purpose is to inform users: employees, contractors, and other authorized individuals of their obligations for protecting the technology and information assets of BMSG. It describes the assets that we must protect and identifies the most common threats to them. It also describes the user's responsibilities and privileges: *'What is considered acceptable to use'*, and *'What are our Rules regarding Internet interactions'*. It also describes user limitations and potential penalties for violation of the policies we have set in place to restrict, monitor, control, and secure such assets. In documenting procedures for responding to incidents that threaten security of BMSG computer systems and networks, BMSG also demonstrates our commitment to all clients, vendors, and other stakeholders in realising how we respect all outward an inward facing utilisation of sensitive data.

# Protection

It is the obligation of all users of BMSG systems to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft, sabotage, manipulation, and destruction. The technology and information assets of the company are made up of the following components:

- Computer hardware, CPU's, disc's, Email, web-based sites and interactions, application servers, PC systems, application software, system software, etc.

- System Software including operating systems, database management systems, LIMS, and backup and restore software, communications protocols, etc.

- Application Software: used across BMSG. This includes custom written software applications, and commercial off the shelf software packages.

- Communications Network hardware and software including routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

## Information Classification

User information found in computer system files and databases is classified as either confidential or non-confidential. As BMSG shall classify all information flowing in and out of its doors BMSG has set in place a requirement to review and approve the classification of the information to determine the appropriate level of security to best protect it. Furthermore, classification of information controlled by 3rd parties not administered by BMSG may be scrutinised under the auspices of Due Diligence.

In order classify data safety and security requirements we have adopted our common Risk Assessment Strategy used for all other processes and related it to Information Security. Below are the 4 levels we have set:

1. RED: This system contains confidential information – information that cannot be revealed to personnel outside of the company. Even within the company, access to this information is provided on a "need to know" basis.

The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of the company.

An example of this is: Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information.

2. ORANGE: This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.

An example of this is: User department PCs used to access Server and application(s). Management workstations used by systems and network administrators.

3. YELLOW: This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.

An example of this is: A test system used by system designers and programmers to develop new computer systems.

4. GREEN: This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information.

An example of this is: A public Web server with non-sensitive information.

# Threats

## Personnel

One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. In order to mitigate for such BMSG has incorporated the following:

- Only give out appropriate rights to systems. Limit access to only business hours.
- Impose ID and password protection on all systems and access points.
- Include IT overview and training modules to support some simple key take home messages:
  - Expect that personnel do not share accounts to access systems.
  - Trust personnel never share your login information with co-workers.
- When separated or disciplined, your access to systems is removed or limited.
- Vigilance from employees to respect that the system is advanced with detailed system logs for login-logout-delete allowing system access and utility traceability for performance and threat metrics.
- Respect that there is a requirement for business continuity, safety and security associated with administration of device, equipment, workflow, IT, data, PPPI access and responsibility across all activities of BMSG; including their own PPPI.
- Demonstrate system utility by physically securing computer assets so that they are only accessible at appropriate times, by appropriate users.

## Hackers and Vandals

Amateur hackers and vandals are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be many attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favourite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness, they are likely to move on to an easier target.

## Saboteurs

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

BMSG has set out a series of automated traceability and performance logs from several systems related to data transfer, storage, deletion therein; generating log files for management, DPO, QAM and IT to monitor performance, identify for non-conformities and detect possible security breaches.

# User Responsibility

## Acceptable Use

User accounts on BMSG computer systems are to be used only for business of the company and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of BMSG computing system and facilities may constitute grounds for either civil or criminal prosecution.

- Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of BMSG.

- Users shall not purposely engage in activity with the intent to:
    - harass other users.
    - degrade the performance of the system.
    - divert system resources to their own use.
    - or gain access to BMSG systems for which they do not have authorization.
- Users shall not attach unauthorized devices on their PCs or workstations unless they have received specific authorization from the management or BMSG-IT/DPO designate.
- Users shall not download unauthorized software from the Internet onto their PCs or workstations.
- Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

## Internet Use

The company will provide Internet access to employees and contractors who are connected to the internal network and who has a business need for this access. Employees and contractors must obtain permission and file a request with the IT/DPO.

The Internet is regarded as an integral and sensitive business tool. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for “chain letters” or any other purpose which is illegal or for personal gain.

## User Classification

All users are expected to have knowledge of BMSG security policies and are required to report violations to management. BMSG has established the following user groups and defined the access privileges and responsibilities:

- Personnel: Access to application and databases as required for job function. (RED and/or GREEN cleared).
- Administrators: Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a “***need to know***” basis only.
- IT: Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
- Programmer: Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
- Consultant/Contractor: Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to company information and systems must be approved in writing by the company director/CEO.
- Partners: Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.
- General Public: Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information.

## Monitoring

BMSG reserves the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not BMSG policy or intent to continuously monitor all computer usage by employees or other users of BMSG computer systems and networks. However, users of the systems should be aware that the company may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g., site accessed, on-line length, time of day access), and employees’ electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with BMS policies.

# Access Control

A fundamental component of our Cyber Security Policy is controlling access to critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by *logon ID* and *password*. At the application and database level, other access control methods have been implemented to further restrict access. Administration level permissions are utilised to limit unauthorised access based on tasks.

## Normal User Identification

Your account access will require a unique *logon ID* and *password*. Your user’s password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

• Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard “hacker tools”.

• Passwords should not be posted on or near computer terminals or otherwise be readily accessible around the terminal; or for that matter be located outside of a Password Manager that does not maintain similar password level restrictions.

• Password must be changed following yearly QMS review.

• Your accounts will be frozen after 3 failed logon attempts.

• Your *logon IDs* and *passwords* will be suspended after 30 days without use.

• You are not allowed to access password files on any network infrastructure component.

• Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

• You are not allowed to logon as a System Administrator, without managerial authorisation. Users who need this level of access to production systems must request a Special Access account.

• Your *logon IDs* and *passwords* will be deactivated as soon as possible if you are terminated, fired, suspended, placed on leave, or otherwise depart the employment of BMSG.

• Supervisors /Managers shall immediately and directly contact the company IT Manager to report any change in your status that requires terminating or modifying your logon access privileges.

• If you forget your password, IT must be informed to obtain a replacement.

• You are responsible for all transactions occurring during Logon sessions initiated.

• You should not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

## Administrator Access

System Administrators, network administrators, and security administrators will have relevant access to host systems, routers, hubs, and firewalls as required to fulfil the duties of the nominated task.

All system administrator passwords will be DELETED immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of BMSG.

## Special Access

Special access accounts are provided to if you require temporary system administrator privileges to perform a task. These accounts are monitored by BMSG and require the permission of the DPO/IT and management. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire upon completion of the task.

### 3rd Party Connection

BMSG is aware of the potential threats such connection may entail. "Third-party" refers to vendors, consultants and business partners. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of said company. The third-party company will ensure that only authorized users will be allowed to access information on the BMSG network. The third-party will not allow Internet traffic, or other private network traffic to flow into the network.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet our requirements they will be re-designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved following appropriate risk assessment.

### Network Connection

Only authorized devices may be connected to BMSG network(s). Authorized devices include PCs and workstations owned by BMSG that comply with our configuration guidelines. Other authorized devices include network infrastructure devices used for network management and monitoring; or those legally binding.

Users shall not attach to the network: non-BMSG computers that are not authorized, owned and/or controlled by BMSG. This includes but not limited to WIFI accessibility.

You should observe caution in your selection of functions, sites, tools, downloads, or other content that you interact with once logged in through a BMSG connectivity point. Your actions and possible consequences thereof are clearly outlined in other BMSG policies.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g., thumb drives or writable CD's; or any other potential corruptive device or software that could compromise BMSG safety and security.

### Remote Access

Only authorized persons may remotely access the BMSG network. Remote access is provided to those employees, contractors and business partners of BMSG that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to BMSG network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID, according to our relevant policies.

### Unauthorised Remote Access

The attachment of any hardware to a user's PC or workstation that is connected to BMSG LAN is not allowed without the written permission. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

## Penalties

BMSG takes the issue of security seriously. Those who use the technology and information resources of BMSG must be aware that they can be disciplined if they violate this or any of our policies. Upon violation, YOU may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies and the BMSG QMS.

In a case where the accused person is not an employee of company the matter shall be submitted to our legal for consideration as to whether criminal charges should be filed against the alleged violator(s).

## Security Incident Handling

BMSG provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the BMSG network. Some examples of security incidents are:

- Illegal access of a BMSG computer system, e.g., hacker logs onto a production server and copies the password file.
- Damage to a BMSG computer system or network caused by illegal access, e.g., releasing a virus or worm.
- Denial of service attack against a BMSG web server, e.g., hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of BMSG network, e.g., system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

If you believe a terminal or computer system has been subjected to a security incident, or has otherwise been improperly accessed or used, you should report the situation to management immediately. You should not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.