PHYSICAL SECURITY POLICY

BMI Group Physical Security Policy
Effective: June 16, 2022

1. Intent

The purpose of this policy is to define the physical security standards necessary to meet BMI Group's ("BMI" or the "Company") obligation to safeguard its personnel, facilities (including managed offices and sites), and information. This policy supports the Company's efforts to comply with the EU General Data Protection (the "GDPR"), and where applicable local data protection legislation's, requirement that organizations implement appropriate technical and organizational measures to prevent the loss of or unauthorized access to Personal Data, as defined in section 4 below.

2. Policy

BMI is responsible for the security and protection of its personnel, facilities and information. The Company utilizes its collective resources and integrates administrative, financial, information security, operational, personnel, procedural, and technical components to meet this requirement. Successful security protection dictates BMI locations have physical control of their overall facility, including sensitive information (in physical and digital forms), and restricted space that contains related data including major computer and telecommunications resources.

BMI's information is expansive in physical forms that include both paper and electronic media, all of which must be protected in accordance with governing requirements. Regarding Personal Data, BMI collects, stores, handles, transports and processes information that relate to the privacy of citizens and its core business activities.

Therefore it is imperative that BMI protects its personnel, facility and information from harm, including the risk and magnitude of loss that could result from intentional or unintentional acts or events, inadvertent or deliberate disclosure, alteration or destruction of property and/or sensitive information. All related material must be protected in accordance with prescribed standards to prevent harm or loss from theft, unauthorized disclosure or misuse.

While every BMI location may not meet the physical security standards outlined below, BMI Group will work with the relevant functional business owner and others to develop acceptable short and long-term mitigation strategies to meet the needs delineated herein.

Policy Exception – Any requests for exception to this policy must to be submitted to the Chief Operating Officer delineating the necessity for the deviation. Exceptions are interim measures to afford sufficient time and latitude to meet the intention of the policy. The Chief Operating Officer will consult the General Counsel, or his/her designee, to either approve or deny temporary exceptions and thereafter monitor and track for compliance.

This policy is supplementary to any local regulatory or statutory obligations. Where local laws and/or regulations are more stringent than those outlined herein, those controls will prevail. Escalate potential conflicts to the General Counsel.

3. Responsibilities

BMI business units and facilities are responsible for coordinating the physical security protections of their critical resources and, as such, it is essential that every reasonable precaution be used to safeguard Company personnel, facilities, and information.

Accordingly, each BMI location and its site manager are responsible for ensuring:

- the security measures outlined in this policy are implemented;
- that there is a named individual responsible for physical security at each BMI Location; and
- annual physical security assessments are completed in a timely fashion.

4. Definitions: site manager - BMI designee (local BMI manager or someone with responsibility for physical security; 3rd party warehouse have access to customer files)

- **Data Room:** Location used for housing data, usually of a secure or privileged nature e.g. physical data rooms, virtual data rooms, or data centers. It is used for a variety of purposes, including data storage, document exchange, file sharing, financial transactions, legal transactions, and more.

- **Personal Data:** any information related to an identified or identifiable natural person, and in the event that the Protection of Personal Information Act 4 of 2013 ("**POPIA**") applies, an identifiable, existing juristic person ("**data subject**"). An identifiable natural person and/or juristic person (where applicable) is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject.

- **Physical Security:** The application of physical barriers, site location, and control procedures as preventive measures or countermeasures against threats to resources and sensitive information. It involves the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee).

- **Sensitive Personal Data:** Personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data, and in the event that POPIA is applicable, the criminal behaviour of a data subject to the extent that such information relates to (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

- **Server Room:** A room used to store, power and operate computer servers and their associated components. This room is part of a data center, which typical houses several physical servers lined up together in different form factors, such as rack mounted, or in tower or blade enclosures

- **Site:** any location out of which BMI conducts operations or business or which serves as the office location for any BMI employee. This includes, but is not limited to, headquarters, offices, sales offices, plant or manufacturing facilities, and distribution centers (including those managed by third parties).
- **Site manager:** the individual designated by BMI as responsible for the overall operations or management of a site. In the case of distributions centers managed by third-parties, the site manager may be designated by such third- party, rather than by BMI, and will be requested to implement this policy with respect to BMI data.

5. BMI Location Security Standards

5.1 PERIMETER SECURITY

The main access to BMI locations should be controlled by smart card access. If, however, that is not feasible and physical keys are used to control entry, only a limited number of keys shall be issued and the site manager or his/her designee shall maintain a key log listing all individuals to whom keys have been issued. All exterior facing doors should remain locked, closed and be equipped with contact alarms.

5.2 RECEPTION AREAS AND ACCESS TO BMI INTERNAL LOCATIONS

The reception area of each BMI location should be equipped with a separate access control (door, access control elevator or other security control) to prevent unauthorized visitors from gaining direct access to the other areas of the facility.

Access cards (preferably electronic) will be provided to each individual at BMI locations, and access to BMI internal locations shall be restricted according to the nature of each individual's business. Access provided must also be reviewed by the individual's manager and/or HR. Photo cards should be issued to BMI employees where possible and should include the individual's name but not BMI name or address. Access or photo cards should be safeguarded by employees, and employees must immediately notify their site manager or his/her designee in the event an access or photo card is lost or stolen. Any employee who forgets his/her pass will be issued a temporary pass for a limited duration. All temporary passes must be surrendered prior to leaving the relevant BMI location.

Each BMI location's site manager or his/her designee shall develop and maintain a list of all individuals permitted on site and shall designate those areas within the site to which each individual has been granted access. The site manager or his/her designee shall reviews the access list semi-annually and shall Immediately remove individuals from the facility access list when access is no longer required.

5.3 VISITORS

All visitors, whether clients, contractors, or vendors, must "sign in" when visiting a BMI location. The following details must be recorded on a log and retained for at least 180 days:

- Date and time of arrival;
- Name of visitor(s);
- Visitor company; and

- Signature.

Visitors must be issued passes that clearly differentiate them from employees either by color or because they are clearly labelled as visitor. Visitors must return all passes on leaving and update the visitor log with a departure time.

Visitors must not be allowed to freely move between non-confidential and confidential areas.

Employees are responsible for ensuring that their visitors remain only within permissible areas

during their visit.

Deliveries or collections must be supervised by a member of the security or reception teams.

5.4 ELECTRONIC SYSTEM SECURE ROOMS

Computers, data servers and telephone equipment will be secured in either a room or appropriate caging. Room or cage access will be physically locked (by physical key or smart pass) and access must be restricted to only those who are authorized to access the electronic equipment. Secure rooms must be locked and alarmed when they are not being used.

Combinations, codes and keys should be changed when keys are lost, combinations or codes are compromised, or individuals are transferred or terminated. Document and thoroughly investigate all anomalous activities including alarm activations and report written findings to the plant manager or designated person.

Servers must not be located where there is likelihood of flooding (below ground level) or where necessary alerts to such events do not exist.

Servers and telephone equipment must have an appropriate uninterrupted power supply (UPS) to manage any unforeseen power issues. For critical infrastructure there must be at least 2 forms of UPS (battery and generator) with enough back-up power for 36 hours.

Third party access to electronic systems is only permitted when directly supervised by a member of BMI staff or security. There should be signage at the entrance to archival storage, file rooms, server rooms and IT equipment rooms, with a warning that access is restricted to authorized personnel (listing the point of contact). There should also be a sign noting that food, drink, and smoking is prohibited while therein.

5.5 PHYSICAL DATA PROTECTION

To the extent BMI locations maintain onsite record archive areas, they must be physically locked (physical key or smart pass) when not in active use. Access to archive facilities will be restricted to those that operate it. The site manager shall designate the individual(s) who shall be responsible for maintaining onsite records archives (“Archives Manager”). Any other employee needing access to such area must be admitted by the Archives Manager, who will maintain a log of all individuals who access the archive records area and of all files that are sent or received from the facility.

Generally, Archives Managers should work with the leadership of each functional department at their respective BMI location to create a method by which to inventory and catalogue all paper records maintained at the site. Such inventory should identify ownership for the records, general description of the records and whether such records constitute personal or confidential information. The Archives Manager should consult with the Site Manager and the department leaders to determine what records should be maintained in an archive records area and which records should be maintained in local workspaces, as necessary to meet the business needs of that site and each function.

Regarding Personal Data kept at BMI locations, BMI Site Managers and Archives Managers should identify the departments and functional areas most likely to create and store records containing Personal Data and sensitive information. The Site Manager should take all necessary measures to restrict access to paper files containing Personal Data and sensitive information to those with a specific need.

All records that contain personal or confidential information must be stored in a secure manner for example in a lockable cabinet or secure room. These records should be protected at all times and should not be left in/on office desks, copiers, printers or open work spaces. These records should not be removed from the site unless authorized by the Site Manager and must remain secured at all times in order to prevent theft or loss. For example, such files should not be left in cars, hotels or other public locations.