BERGRIVIER MUNICIPALITY

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

APRIL 2012

1. SECURE AREAS

Objective: To prevent unauthorised access, damage and interference to business premises and information.

It is essential that critical information processing facilities are housed in secure areas, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference, commensurate with the identified risks. The practices of “clear desk” and “clear screen” should be encourage to reduce the risk of unauthorized opportunist access to facilities.

1.1 PHYSICAL SECURITY PERIMETER

Physical protection must be implemented through one or more physical barriers around the information processing facilities. Each barrier establishes a security perimeter, each increasing the total protection provided.

The following guidelines and controls will be considered and implemented where appropriate:

(a) security perimeters are to be clearly defined;

(b) the perimeter of buildings or sites housing information processing facilities must be physically sound, i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur;

(c) a manned reception area or other means to control physical access to the site or building should be in place;

(d) access to sites and buildings should be restricted to authorized personnel only; and

(e) where necessary, physical barriers should extend from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire or flooding.

1.2 PHYSICAL ENTRY CONTROLS

Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following controls will be implemented as appropriate:

(a) visitors to secure areas must be supervised or cleared and their date and time of entry and exit recorded. Visitor access will only be granted for specific, authorized purposes and the visitor must be advised of the relevant security requirements pertaining to the area, and the applicable emergency procedures, if any;

(b) access to sensitive information, and information processing facilities, shall be restricted to authorized persons only; and

(c) staff working at secure sites must be instructed to challenge unescorted strangers and anyone not displaying visible identification.

1.3 SECURING OFFICES, ROOMS AND FACILITIES

A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of secure areas must take into account the possibility of damage from fire, flood, explosion, civil unrest, and other forms of natural or manmade disaster. Consideration must also be given to any security threats posed by neighboring premises, e.g. leakage of water from other areas.

The following controls will be considered and implemented as appropriate:

(a) Key facilities must be sited so as to avoid or at least minimize access by the public;

(b) Buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities;

(c) support functions and equipment, e.g. photocopiers, fax machines, etc. must be sited appropriately within the secure area to avoid demands for access that could compromise information;

(d) doors and windows must be locked when unattended and additional protection (e.g. burglar bars) provided for windows, particularly at ground level;

(e) directories and internal telephone books identifying locations of sensitive information processing facilities must not be readily accessible to the public;

(f) hazardous or combustible materials must be stored securely at a safe distance from a secure area. Bulk stationery supplies must not be located within a secure area until required; and

(g) fallback equipment and backup media must be sited at a safe distance to avoid damage from a disaster at the main site.

1.4 WORKING IN SECURE AREAS

Additional controls and guidelines may be required to enhance the security of a specific secure area, viz. in respect of staff or third-parties working in the secure area, or third party activities taking place there. Where appropriate, the following controls will be implemented:

(a) staff should only be aware of the existence of, or activities within, a secure area on a need to know basis;

(b) unsupervised working in secure areas should be avoided, both for safety reasons and to prevent opportunities for malicious activities;

(c) vacant secure areas must be locked and checked periodically;

(d) third party support services staff should only be granted access to secure areas or sensitive information for specific purposes and at specific times. This access must be appropriately authorized and monitored; and

(e) photographic, video, audio or other recording equipment (including camera/video equipped cellular phones) should not be allowed inside secure areas without proper authorization.

2. EQUIPMENT SECURITY

Objective: To prevent loss, damage, or compromising of assets and interruption to business activities.

Equipment must be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site, e.g. notebook computers) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also consider siting and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

2.1 EQUIPMENT SITING AND PROTECTION

Equipment must be sited or protected to reduce risks from environmental threats and hazards, and opportunities for unauthorized access. The following controls must be considered:

(a) equipment must be sited to minimize unnecessary access into work areas;

(b) information processing and storage facilities handling sensitive data must be positioned to reduce the risk of overlooking during their use;

(c) items requiring special protection must be isolated to reduce the general level of protection required;

(d) potential threats:

(i) theft;
(ii) fire;
(iii) explosives;
(iv) smoke;
(v) water (or supply failure);
(vi) dust;
(vii) vibration;
(viii) chemical effects;
(ix) electrical supply interference (or supply failure); and
(x) electromagnetic radiation;

(e) smoking is generally covered by applicable legislation: where this may be interpreted as not being applicable, smoking in the proximity of information processing facilities is expressly prohibited;

(f) over and above provisions that may be contained in the Conditions of Service, the use of alcohol (or other forms of substance abuse) in secure areas or in the proximity of information processing facilities is expressly prohibited;

(g) consumption of food or beverages in secure areas or in the proximity of information processing facilities should be discouraged where possible;

(h) environmental conditions that could adversely affect the operation of information processing facilities must be monitored; and

(j) the impact of a disaster happening in nearby premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street should be considered.

2.2 POWER SUPPLIES

Key equipment must be protected from power failures and other electrical anomalies. A suitable electrical supply conforming to the equipment manufacturer's specifications must be assured. To do so may require one or more of the following:

(a) multiple feeds to avoid a single point of failure in the power supply;

(b) uninterruptible power supply (UPS); and/or

(c) backup generation facilities.

A UPS to support orderly shutdown or continuous running is necessary for equipment supporting business-critical operations. Contingency plans must cover the action to be taken in the event of failure of the UPS. UPS equipment must be regularly checked to ensure adequate capacity and tested in accordance with the manufacturer's recommendations.

A backup generator should be considered if processing must continue in case of prolonged power outage. If installed, procedures must be implemented to regularly test generators in accordance with the manufacturer's recommendations. An adequate supply of fuel should be available to ensure that the generator can function for prolonged periods. Due consideration must be taken when siting such facilities, particularly with regard to fuel supply and replenishment thereof, to minimize possible risks to information processing facilities.

2.3 CABLING SECURITY

Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage. The following controls should be considered:

(a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;

(b) network cabling should be protected from unauthorized interception, or damage, through for example the use of conduit or by avoiding routes through public areas;

(c) power cables should be segregated from communications cables to prevent electromagnetic interference; and

(d) for sensitive or critical systems, further controls to consider include:

(i) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

(ii) use of alternative routings or transmission media;

(iii) use of fibre optic cabling; and

(iv) initiation of sweeps for unauthorized devices being attached to cables.

2.4 EQUIPMENT MAINTENANCE

Equipment must at all times be correctly maintained to ensure continued availability and integrity, compliance with warranty provisions and protection of the municipality's investment. The following controls must be considered:

(a) equipment must be maintained in accordance with the manufacturer's recommendations according to the manufacturer's recommended service intervals and specifications;

(b) only authorized maintenance personnel may carry out repairs and service equipment;

(c) records should be kept of all suspected or actual faults and all preventive and corrective maintenance; and

(d) appropriate procedures and controls must be applied when equipment leaves Municipal premises for maintenance (in particular, the confidentiality and security of data that may be stored in the equipment must be considered).

2.5 SECURITY OF EQUIPMENT OFF-PREMISES

Regardless of ownership, the use of any equipment outside of municipal premises for information processing should be authorized by management particularly when access to the municipal network or servers is available via such equipment. The security provided should be equivalent to that for on-site equipment used for the same purpose, taking into account the risks associated with working outside the municipality's premises. Information processing equipment includes all forms of personal computers, personal digital assistants (PDAs), organizers, mobile phones, paper or other form, which is held for home working or being transported away from the normal work location. The following controls must be considered:

(a) equipment and media taken off the premises must not be left unattended in public places. Portable computers should be carried as hand luggage on aircraft and disguised where possible when travelling. Under no circumstances should equipment be left in view in a vehicle;

(b) manufacturer's instructions for protecting equipment against exposure to strong electromagnetic fields, heat, etc. must be observed at all times; and

(c) any insurance cover implications need to be addressed.

2.6 SECURE DISPOSAL OR RE-USE OF EQUIPMENT

Information security can be compromised through careless disposal or re-use of equipment. Storage devices containing sensitive information should be physically destroyed or securely overwritten, rather than simply using the standard 'delete' function which effectively resets the file size to zero without destroying the data. In cases of extreme sensitivity, it may be necessary to overwrite the disk up to seven times to ensure that the data is unrecoverable.

Final disposal of information processing equipment, in common with all municipal movable assets, is subject to the provisions of the Asset Management Policy.

3. GENERAL CONTROLS

Objective: To prevent compromising or theft of information and information processing facilities.

Information and information processing facilities must be protected from disclosure to or modification by unauthorized persons, or theft. Effective controls must be implemented to minimize the risk of loss or damage.

3.1 CLEAR DESK AND CLEAR SCREEN POLICY

It is recommended that "clear desk" and "clear screen" practices become the norm at all municipal premises, so that removable media and information contained in paper reports are not visible or accessible to unauthorized persons. Information storage media left on desks is also more likely to be damaged in the event of a disaster such as fire, flood or explosion. The following controls should be considered and implemented where appropriate:

(a) paper documents and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside of working hours;

(b) sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated;

(c) personal computers and computer terminals must not be left logged on when unattended and should be protected by key locks, screensavers with passwords or other controls when unattended; and

(d) sensitive or classified information, when printed, should be cleared from printers immediately. Persons who regularly need to print such documents should consider a personal printer rather than using shared facilities, where appropriate.

3.2 REMOVAL OF PROPERTY

Equipment, information or software must not be taken off-site without proper authorization. Where necessary and appropriate, equipment should be logged out and logged back in when returned. Spot checks should be undertaken at random to detect unauthorized removal of property. Staff should be made aware that such spot checks will be conducted.