[Company Name]

Facility Security Plan

I. Introduction

This facility security plan describes the methods, procedures and measures to be used by [Company Name] in order to establish security measures and prevent loss, damage or compromise of assets and interruption to business activities.

A risk assessment was performed in order to assess security risks to equipment, facilities, and data storage, transmission and processing activities, and is attached in the Appendix.

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

[Company Name] currently operates (data centers, networks, other systems). The (data centers, networks, other systems) support (operations, # users, locations).

(Other operating parameters of data centers, networks, other systems)

(Current security capabilities)

(Vendor capabilities, if security was outsourced)

(Summary of Facility Security Plan – measures, vendors, budget/cost, people)

II. Equipment location and protection

Equipment should be located or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. The following controls should be considered.

A. Equipment should be located to minimize unnecessary access into work areas.
B. Information processing and storage facilities handling sensitive data should be positioned to reduce the risk of overlooking during their use.
C. Items requiring special protection should be isolated to reduce the general level of protection required.
D. Controls should be adopted to minimize the risk of potential threats including:
    1. theft;
    2. fire;
    3. explosives;
    4. smoke;
    5. water (or supply failure);

6. dust;
7. vibration;
8. chemical effects;
9. electrical supply interference;
10. electromagnetic radiation.

E. An organization should consider its policy towards eating, drinking and smoking on in proximity to information processing facilities.
F. Environmental conditions should be monitored for conditions which could adversely affect the operation of information processing facilities.
G. The use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments.
H. The impact of a disaster happening in nearby premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in the street should be considered.

III.Power supplies

Equipment should be protected from power failures and other electrical anomalies. A suitable electrical supply should be provided that conforms to the equipment manufacturer's specifications.

Options to achieve continuity of power supplies include:

A. multiple feeds to avoid a single point of failure in the power supply;
B. uninterruptable power supply (UPS);
C. back-up generator.

A UPS to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Contingency plans should cover the action to be taken on failure of the UPS. UPS equipment should be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

A back-up generator should be considered if processing is to continue in case of a prolonged power failure. If installed, generators should be regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period.

In addition, emergency power switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure. Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all external communications lines.

IV. Cabling security

Power and telecommunications cabling carrying data or supporting information services should 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, for example by using conduit or by avoiding routes through public areas.

C. Power cables should be segregated from communications cables to prevent interference.
D. For sensitive or critical systems further controls to consider include:
    1) installation of armored conduit and locked rooms or boxes at inspection and termination points;
    2) use of alternative routings or transmission media;
    3) use of fiber optic cabling;
    4) initiation of sweeps for unauthorized devices being attached to the cables.

V. Equipment maintenance

Equipment should be correctly maintained to ensure its continued availability and integrity. The following controls should be considered.

A. Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.
B. Only authorized maintenance personnel should carry out repairs and service equipment.
C. Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.
D. Appropriate controls should be taken when sending equipment off premises for maintenance. All requirements imposed by insurance policies should be complied with.

VI. Security of equipment off-premises

Regardless of ownership, the use of any equipment outside an organization's premises for information processing should be authorized by management. The security provided should be equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside the organization's premises. Information processing equipment includes all forms of personal computers, organizers, mobile phones, paper or other form, which is held for home working or being transported away from the normal work location.
The following guidelines should be considered:

A. Equipment and media taken off the premises should not be left unattended in public places. Portable computers should be carried as hand luggage and disguised where possible when traveling.
B. Manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields.
C. Home-working controls should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, and access controls for computers.
D. Adequate insurance cover should be in place to protect equipment off site.
E. Security risks, e.g. of damage, theft and eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

VII. Secure disposal or re-use of equipment

Information 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 using the standard delete function.

All items of equipment containing storage media, e.g. fixed hard disks, should be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to

disposal. Damaged storage devices containing sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.