buzzsaw MEDIA

Physical Environment Security

1. Introduction

1.1 Scope

This document sets out Buzz Saw's arrangements for:

- Preventing unauthorised physical access, damage, and interference to our information and information processing facilities
- Preventing loss, damage, theft or compromise of assets
- Preventing interruption to our operations

1.2 Revision History

Revision	Date	Record of Changes	Approved By
0.0	01/01/2020	Initial Issue	JE/WS

1.3 Control of hardcopy versions

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this manual is uncontrolled, and cannot be relied upon, except when formally issued by the ISMS Manager and provided with a document reference number and revision in the fields below:

Document Ref	Rev.	Uncontrolled Copy	X	Controlled Copy

1.4 References

Standard	Title	Description
SO 27000:2014	information security management systems	Overview and vocabulary
SO 27001:2013	information security management systems	Requirements
ISO 27002:2013	information technology-security techniques	Code of practice for information security controls
ISO 27001:2013	information security management systems	Clause A.11 Physical and environmental security

1.5 Terms and Definitions

“staff” and “users” means all of those who work under our control, including employees, contractors, interns etc.
“we” and “our ”refer to Buzz Saw

1.6 Responsibilities

The ISMS Manager is jointly responsible with the Facilities Manager for all aspects of the implementation and management of these arrangements, unless noted otherwise.

Managers and supervisors are responsible for the implementation of these arrangements within the scope of their responsibilities and must ensure that all staff under their control understand and undertake their responsibilities accordingly.

2. Secure Areas

Where appropriate, we provide secure areas to prevent unauthorised physical access, damage, and interference to our information and information processing facilities.

2.1 Physical security perimeter

Security perimeters have been defined and are used to protect areas that contain either sensitive or critical information and information processing facilities.

Physical security perimeters, including barriers such as walls,card-controlled entry gates, or manned reception desks, are implemented taking into account the following guidelines:

- Security perimeters are to be clearly defined, and the siting and strength of each perimeter should reflect the security requirements of the assets within the perimeter and the results of a risk assessment.
- Perimeters of the building or site containing information processing facilities must be physically sound and all external doors must be protected against unauthorized access with control mechanisms.
- Where necessary, doors and windows are to be locked when unattended and external window protection (grills) provided, particularly at ground level.
- The reception area is to be manned and access to sites and buildings should be restricted to authorized staff only where necessary, physical barriers are to be erected to prevent unauthorized physical access and environmental contamination.
- All fire doors on the security perimeter are to be fitted with alarms, monitored, and tested to establish the required level of security in accordance with appropriate standards -fire doors must always operate in accordance with the applicable fire code in a failsafe manner.
- Insurer approved or recommended intruder detection systems are to be installed and regularly tested to cover all external doors and accessible windows.

- Computer rooms, communications rooms and unoccupied areas are to be alarmed at all times.
- Information processing facilities that we manage are to be physically separated from those managed by third parties.

2.2 Physical entry controls to secure areas

Secure areas are protected by appropriate entry controls to ensure that only authorised staff are allowed access.

The date and time of entry and departure of visitors to secure areas are recorded and all visitors are supervised unless their unsupervised access has been previously approved. Visitors are only granted access for specific authorised purposes and are briefed, in advance, on the security requirements of the area and on emergency procedures.

Authentication controls (access control card plus PIN to be entered at the door or similar)are used to authorize and validate all access. An audit trail of all access is securely maintained.

All employees, contractors, and visitors are required to wear some form of visible identification. All employees, contractors and visitors are required to immediately notify security staff if they encounter unescorted visitors and anyone not wearing visible identification.

Third-party support service staff are granted restricted access to secure areas only when required, and this access is authorised and monitored.

Access rights to secure areas are regularly reviewed and updated and revoked when necessary.

2.3 Securing offices, rooms and facilities

Physical security for offices, rooms, and facilities have been designed and applied taking into account the following guidelines:

- All relevant health and safety and fire regulations must be observed.

- Where practicable, key secure facilities are to be sited so as to avoid access by the public.
- Internal directories and plans identifying locations of sensitive information processing facilities are to be kept away from the public
- Where practicable, buildings and facilities are to be made unobtrusive and give a minimum indication of their purpose, with no obvious signage identifying the presence of information processing activities.

2.4 Protecting against external and environmental threats

Appropriate physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster have been put in place, taking into account the following guidelines:

- Hazardous or combustible materials are stored at a safe distance from a secure area.
- Where practicable, key secure facilities are to be sited so as to avoid access by the public.
- Bulk supplies such as stationery are not stored within a secure area.
- Backup equipment and media are sited at a safe distance from the location where they would be used.
- Appropriate fire-fighting equipment is provided in suitable locations, and staff appropriately trained, in accordance with our fire risk assessment and fire safety policy.

2.5 Working in secure areas

We have established information security policies and procedures to be followed by staff working in secure areas.

- Staff are made aware of only the existence of, or activities within,a secure area on a need to know basis.
- Unsupervised working in secure areas is avoided both for safety reasons and to limit opportunities for malicious activities.
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices are not permitted in secure areas unless authorized.

2.6 Delivery and loading areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, where practicable, isolated from information processing facilities to avoid unauthorized access.

2.7 Visitor Access

Visitors to Buzz Saw offices must:

- Be accompanies at all times by an authorized access entry staff
- Provided access to Visitor rooms (holding no information assets) as a preference
- Limited in all activities by the Access Control Policy
- Not have access to secure offices.

3. Equipment

3.1 Equipment siting and protection

Where practicable, equipment is sited and protected to reduce the risks from environmental threats and hazards.

We reduce the risks and opportunities for unauthorized access by adopting the following measures, wherever practicable:

- Equipment should be sited to minimize unnecessary access into work areas.
- The viewing angle of information processing facilities handling sensitive data should be restricted to reduce the risk of information being viewed by unauthorized persons.
- Storage facilities should be secured to avoid unauthorized access.
- Items requiring special protection should be isolated to reduce the general level of protection required.
- Controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply

failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.
- Environmental conditions, such as temperature and humidity, should be monitored.
- Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines.

3.2 Supporting utilities

We protect critical equipment from power failures and other disruptions caused by failures in supporting utilities.

The precautions we employ, where appropriate and practicable, include:

- Incoming support utilities are regularly inspected and tested as appropriate.
- An online UPS system having adequate backup time has been installed to support orderly close down or continuous running for equipment supporting critical business operations.
- Power contingency plans cover the action to be taken on the failure of the UPS. A backup generator has been installed and an adequate supply of fuel is made available to ensure that the generator can perform for a prolonged period.
- The UPS and generator are maintained and checked regularly to ensure there is adequate capacity.
- Emergency power-off switches are located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency.
- Emergency lighting is provided in case of main power failure.
- An alarm system detects malfunctions in the supporting utilities.
- Telecommunications equipment are connected to the utility provider by at least two diverse routes to prevent failure in one connection.
- Voice services are adequately protected to ensure their continued functioning for emergency communications.

3.3 Cabling security

Power and telecommunications cabling carrying data or supporting information services are installed in such a way that they are protected from interception or interference or damage.

The precautions we employ, where appropriate and practicable, include:

- Power and telecommunications lines into information processing facilities are situated below ground, or subject to adequate alternative protection.
- Network cabling is protected from unauthorised interception or damage, by using a conduit (shield) or by avoiding routes through public areas.
- Power cables are segregated from communications cables to prevent interference.
- Clearly identifiable cable and equipment markings are used to reduce handling errors.
- A documented patch list is used to reduce the possibility of errors.
- For sensitive or critical systems further controls are used, including:

  – Installation of armoured conduit and locked rooms or boxes at inspection and termination points

  – Use of alternative routings and/or transmission media providing appropriate security

  – Use of fiber optic cabling

  – Use of electromagnetic shielding to protect against interference

  – Initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables

  – Controlled access to patch panels and cable rooms

3.4 Equipment maintenance

We ensure that all equipment is properly maintained to ensure continued availability and integrity, including:

- Equipment is maintained in accordance with the supplier's recommended service intervals and specifications and, where appropriate, preventative maintenance is undertaken.
- Only authorized maintenance staff are permitted to carry out repairs and service equipment.
- Records are maintained of all suspected or actual faults, and all preventive, regular and breakdown maintenance.
- Appropriate controls are implemented when equipment is scheduled for maintenance, including, where necessary, removing information from the equipment prior to maintenance.
- Where additional requirements are made by insurance providers, those requirements are met.

The Facilities Manager maintains an ISMS Routine Maintenance Register, listing appropriate maintenance requirements and schedules, and ensures that such maintenance is carried out in a timely manner.

3.5 Removal of assets

Equipment, information and software are not permitted to be removed from our premises or from secure areas without prior authorisation.

3.6 Security of equipment off-premises

Security has been applied to off-site assets such as laptop computers and GPS systems, taking into account the various additional risks arising from working outside of our premises.

The use of any information processing equipment outside of our premises must be authorised in advance and staff are required to:

- Not leave media or equipment unattended in public places.

- Carry portable devices as hand luggage when traveling.
- Take care not to expose devices to adverse environments, such as water and strong electromagnetic fields.

3.7 Secure disposal or re-use of equipment

All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been thoroughly removed or securely overwritten prior to disposal or re-use.

3.8 Unattended user equipment

All users are made aware of the security requirements for protecting unattended equipment, as well as their responsibilities for implementing such protection.

3.9 Clear desk and clear screen policy

We operate a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

In addition:

- Sensitive or critical business information in physical form is locked away (in a safe or cabinet or other forms of security furniture) when not required or when an office is vacated.
- Facsimile machines are protected from unauthorized use.
- photocopiers and other reproduction technology (e.g., scanners, digital cameras) are protected from unauthorized us
- Documents containing sensitive or classified information are removed from printers immediately.

4. Records

Records retained in support of this procedure are listed in the ISMS Controlled Records Register and controlled according to the Control of Management System Records Procedure.