Physical Security Policy

Version 1.0

19th August 2020

Author: Ben Glasgow (Director)

TABLE OF CONTENTS

1. STATEMENT

The security and protection of Tweed Valley Distilling Company Ltd. assets, facilities, personnel and authorised visitors is fundamental to the effective, efficient and profitable working of the Company.

This Policy provides a framework which allows us to manage resources in the most secure way.

Security is everyone's responsibility and all personnel working in the Company must make every effort to comply with this Policy.

2. SCOPE OF POLICY

2.1 THE NEED

To meet legal and professional requirements the Company must use cost effective security measures to safeguard its physical resources.

This Physical Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

2.2 THE POLICY

The Policy of the Company is to accept willingly all obligations in respect of physical security and to protect its resources by implementing practices that will achieve a balance between cost and risk.

2.3 APPLICABILITY

The Policy shall apply to all employees of and authorised visitors (e.g. couriers, suppliers) to the Company and any other professional using Company resources at the premises.

2.4 IMPLEMENTATION

The requirements of the Policy shall be implemented by all employees, staff and other professionals using the Company's resources.

Ben Glasgow will be responsible for the routine periodic review of the Policy.

Compliance with the Policy is the duty of all employees and authorised visitors.

2.5 RESOURCES

The Policy applies to any resource, whether material, information, or human, which is owned, held in the custody of, used by, or employed within the Company.

3. OBJECTIVES OF THE POLICY

The objectives of the Policy are to ensure that:

- Resources are protected from accidental or malicious damage, and from theft.
- Security risks are properly identified, assessed, recorded and managed.
- Safeguards to reduce risks are implemented at an acceptable cost.
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy.

4. LEGAL OBLIGATIONS

4.1 GENERAL

The Company accepts its obligations to comply with the laws of the United Kingdom.

5. KEY SECURITY CONTROLS

5.1 GENERAL

Ben Glasgow will ensure that all contracts of employment will include a security compliance clause.

Ben Glasgow will ensure that security responsibilities are allocated to employees and written into any job specifications and terms of reference such as may be documented.

Security training will be provided to all staff as appropriate to their assessed needs.

5.2 PHYSICAL SECURITY CONTROL

5.2.1 Principle

Resources associated within the Company, including alcohol products, all other stock, office machinery, IT equipment, other equipment and the area defined as the Premises for the purposes of local authority licencing shall be protected from unauthorised access, misuse, damage or theft.

5.2.2 Access

- All areas of the premises are designated as non-public.
- No person under the age of 18 shall be permitted access to the premises.
- Visitors are to be escorted at all times and a record of visitors will be kept.

5.2.3 Equipment

All assets held by the Company are to be held against an asset register and be uniquely marked as being the property of the Company.

On-going maintenance arrangements are to be made for all essential equipment and installations and are to be reviewed at regular intervals by **Ben Glasgow**

Company equipment, items of stock and other tangible assets are not to be removed from the premises without the authority of **Ben Glasgow.**

5.2.4 Risk Assessment

The Company has a regular process of risk assessment in place to cover all areas of physical security.

Adequate, cost effective controls are to be implemented to reduce the level of associated risk.

5.3 INTERNAL SECURITY CONTROLS

5.3.1 Access Controls

Main door access to the premises is secured by use of a lock and key.

Windows within the premises are secured by use of a lock and key.

The following individuals are issued with keys to access the main premises door and premises windows – **Ben Glasgow**

The following employees are issued with keys to other doors and windows within the wider building which would permit indirect access to the premises: **Ben Glasgow.**

Safe-keeping of all keys controlling access to the premises and the wider building is required to prevent unauthorised access to the premises.

At the end of each working day, it must be ensured that the main door to the premises is fully closed and secured.

At the end of each working day, it must be ensured that the windows within the premises are fully closed and secured.

At the end of each working day, it must be ensured that the premises' internal doors to the wider building are fully closed and secured so as to prevent access by children or young people present within the wider building.

5.3.2 Stock Security

No significant volumes of stock (alcohol), or cash, should be left within the Premises during prolonged periods of time when the premises and wider building are unattended (e.g. holidays.)

Where stock levels at the premises are significant, provision should be made for the transfer of that stock to a suitably secure facility for temporary storage until such time as it can be returned to the premises.

5.3.3 Violence & Aggression

The Company operates a Zero Tolerance Policy toward violence and aggression.

The definition of work related violence is not subjective.

'Violence' means:

'Any incident where staff are abused, threatened or assaulted in circumstances related to their work, involving an explicit or implicit challenge to their safety, well-being or health'.

Violent and abusive behaviour also includes such behaviour over the telephone, social media and other communications channels.

Violence and abuse is **not** part of anyone's duties within the Company.

The Company will not tolerate any violent or abusive behaviour toward its staff and will do all it can to ensure the safety of its staff.

Violence against staff is a crime and the Company will take whatever action is necessary to prosecute offenders

5.4 EXTERNAL SECURITY CONTROL

5.4.1 Access by the Public

Members of the public - including children and young people - are not to be allowed entry to the Company premises under any circumstances.

5.4.2 Outside Areas

The exterior of the building and the Company car park is illuminated by a combination of public street lighting (premises main door) and security floodlights (building rear door.) from dusk until dawn.

No stock, cash or Company resources or assets should be left within vehicles used for Company business overnight under any circumstances – stock and cash should only ever be securely stored within the Company premises.

6. SECURITY INCIDENTS AND REPORTING

A security incident is defined as any event that could result or has resulted in:

1. The integrity of working processes being put at risk.
2. The availability of a resource being put at risk.
3. An adverse impact, for example:
    - Embarrassment to the good business reputation of the Company;
    - Potential jeopardy to terms of Local Authority licencing conditions attached to the Company's trading activities;
    - Threat to personal safety;
    - Legal obligation or penalty;
    - Financial loss;

- Other disruption of activities.

All incidents or information indicating a suspected or actual breach of security must be notified immediately to **Ben Glasgow**.

The types of incidents that can result in a breach of security are many and varied.

Their severity will depend upon a myriad of factors but the majority will be innocent and unintentional and will not normally result in any form of disciplinary action. The likely result will be improved security awareness and mitigation of security risk within the Company.

7. TRAINING

Where identified as a training need, staff training can to be provided covering the following:

- Physical Security
- Dealing with violence and aggression / Conflict resolution
- Risk Assessment

Training when required is to be carried out annually, and will be recorded on staff training records. **Ben Glasgow** is responsible for the arranging all training.

8. POLICY REVIEW

This Policy is to be reviewed on an annual basis by Ben Glasgow to take account of changing circumstances, business operations, on-site resources, legislation, technology and security risks.

Any revisions (major version changes) to this Policy will be lodged with the Scottish Borders Council Licencing Team at the point of implementation.

9. STAFF COMPLIANCE AGREEMENT

All employed and attached staff are to read this Policy and sign and date a copy to confirm agreement to compliance with the Policy.

Signed copies will be retained by the Company**.**

Employee Name

Employee Signature

Signed Date