The Bamford Community Society

IT and Information Security Policy

First produced in	**July 2014**
Updated version approved by	**Directors at meeting on 12.2.2015**
To be reviewed no later than	**January 2016**

1. Policy statement

The Bamford Community Society Ltd is a registered society under the Co-operative and Community Benefit Societies Act 2014 and owned by its members, the majority of whom are residents of the village of Bamford. The Society operates from the Anglers Rest site within Bamford village, in the Derbyshire Peak District and delivers various services for the benefit of residents of Bamford, the wider Hope Valley and visitors to the area. The BCS is a socially responsible business committed to commercial success whilst upholding the highest standards with regards to business operations. This policy forms part of those standards of good practice.

This Information Security Policy:

- Defines the IT and Information Security Policy for the BCS and The Anglers Rest.
- Sets out the BCS's high-level requirements for the management of Information Security in relation to the storage, processing and transmission of confidential data.
- Meets the compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS). Version 3.0, released in November 2013, in particular the standards for merchants with payment application systems connected to the Internet, no electronic cardholder data storage (SAQ C)

This policy should be read in conjunction with the BCS Data Protection Policy

The PCI Data Security Standard specifies 12 requirements for compliance, organized into six logically related groups called "control objectives".

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system password and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

2. IT and Information Security Policy

2.1 Purpose

This document details the IT security strategy for BCS in relation to the storage, processing and transmission of confidential data including credit card data. Its aim is to set out the Information Security responsibilities for staff, contractors, partners and third parties.

As part of The Anglers Rest's Payment Card Industry (PCI) Compliance programme, consideration has been made to Credit Card Processing operations. Guidelines and controls form an essential part of the BCS's compliance status against the PCI Data Security Standard.

This document should be reviewed:

- At least annually when the BCS undertakes its annual PCI compliance review.
- If any new credit card processing or IT systems or processes are implemented.

2.2 Roles and Responsibilities

The Board will identify a lead person, with responsibility for ensuring that the aims set out in this policy document are observed and monitored, together with the reviewing this policy. The BCS IT Security lead may be:

- One of the Directors, who will be provided with appropriate training if required
- A designated manager, again, with training if required
- An IT Security specialist appointed by the Board

The BCS IT Security lead is responsible for:

- Overall responsibility for Information Security and related issues.
- Development and maintenance of Information Security Policies and Procedures
- Communication and review of Information Security Policies.
- Coordination of PCI Security Audit Tasks.
- Coordination with PCI Accredited Security Auditors (Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs))
- Keeping the Board updated on all security related issues.

The Anglers Rest management team are responsible for ensuring that the requirements of this policy are adhered to, including responsibility for

- Ensuring that staff are aware of the IT Security policies and procedures.
- Ensuring that the requirements of the IT Security policies and procedures within their control are adhered to.
- Reporting IT Security incidents or concerns to the IT Security lead and participating in implementing actions where required.

3. IT Security Audits

Regular audits of IT Security will be undertaken, in line with the requirements of the PCI standards, and other standards, as appropriate.

2.3 Annual Policy Review

All Information Security Policies are reviewed and where necessary updated on at least an annual basis. The review process ensures that:

- Policies in place are still required.
- Perceived threats facing the BCS are identified and consideration included in procedural documentation.
- Any new legal issues are identified that require changes in current policy or practice.
- The BCS meets current PCI compliance standards.
- Any changes to network configuration or new applications are included in the security policy.

A formal documented risk assessment process should also be completed annually to identify key business assets (including credit card data stores and supporting networks), and potential threats and vulnerabilities, which could impact on the security of those assets.

2.4 Breaches of this policy

The BCS is committed to ensuring that our IT Security policy is effectively implemented. Any breaches of this policy coming to the attention of management and/or directors will be dealt with appropriately.

2.6 Security Training

All staff will receive security awareness training as part of their induction and at least annually.

The BCS shall also ensure that vendors, contractors, and business partners covered by this policy are familiar with its requirements.

Staff with cardholder data access:
Staff with privileged access, deemed to have the need to know (see PCI DSS Requirement 7) should be given extra training.