1. PCI DSS Compliance Charter

1.1 Purpose

As an organisation that processes, stores and transmits payment card data, CTI has a duty to protect the payment card data in its care at all times.

Operations and networks supporting payment card operations need to be Payment Card Industry Data Security Standard (PCI DSS) compliant. This standard has been developed by the payment card industry to promote secure working practices for the protection of payment card data.

All physical and electronic assets and controls associated with payment card data are formally measured against the standard on an annual basis to assess PCI DSS compliance.

It is important to note that although formal compliance measurement occurs annually, the supporting physical and electronic controls operate in a compliant manner all the time.

CTI has developed this charter as a means of communicating how important payment card data security is. Every effort is made to protect payment card data in its care to avoid instances of fraud and data compromise.

1.2 Structure

CTI's Board has overall responsibility for the security of payment card data in its care.

The Information Security Team has overall responsibility for coordinating all PCI DSS compliance activities.

Specific operational responsibilities are detailed in CTI's Information Security suite of policies and procedures.

1.3 Measurement

PCI DSS Compliance is required to be measured on an annual basis. Measurement, or assessment, takes the form of Self-Assessment and external audit.

Issues arising from assessment are addressed immediately with the goal of achieving full annual PCI DSS compliance.

A PCI DSS Attestation of Compliance (AOC) is then signed and distributed to relevant third parties.

1.4 Responsibilities

To ensure effective protection of payment card data and meet PCI DSS compliance, CTI meets strict physical and logical requirements.

Controls that are enforced include encryption of stored payment card data, secure configuration of protection mechanisms such as firewalls, antivirus and intrusion prevention devices and secure procedures for physical controls such as access to buildings.

All controls and supporting procedures are documented and logged to support accountability and recovery in the event of a data breach or network outage.

CTI accepts its responsibility for security as a custodian of payment card data and will continue to adhere to all applicable controls within the PCI DSS.

2. Issue Status and Distribution

This document is the property of CTI and is updated as necessary to reflect amendments. It is a controlled document and is approved for adequacy prior to issue by the Information Security Team.

This document is reviewed and updated at least annually and re-approved prior to re-issue.

Should there be any alterations to this document a copy of the obsolete document is archived for a period of at least one year and all other obsolete documents are destroyed to prevent their unintended use.

2.1 Document Version

Revision Date	Version No.	Author	Description
06/01/17	0.1	Samantha May	Document creation
18/07/17	0.2	Samantha May	Update template format
20/10/17	1.0	Samantha May	Full review; document finalised
20/07/18	2.0	Samantha May	Full Review

2.2 Document Review

Name	Title	Version	Date
Sue Holmes	Director of IT	2.0	

2.3 Document Approval

Name	Title	Version	Date
Clive Wratten	Chief Executive Officer	2.0	

2.4 Distribution

Where this document is printed and distributed within the organisation a list is kept of all owners in order to control amendments and subsequent recalls. Where copies are supplied to external individuals or organisations these shall be marked as **UNCONTROLLED** at time of issue.

Name	Title	Version	Date of issue
CTI Website	-	2.0	

2.5 Standards

Standard	Reference
PCI DSS v3.2	12.4.1, 12.9

2.6 Glossary of Terms

Term	Definition
AOC	Attestation of Compliance
PCI DSS	Payment Card Industry Data Security Standard