Countrywide
TAX AND TRUST CORPORATION LTD

Gables House
62 Kenilworth Rd
Leamington Spa
Warwickshire CV32 6JX

Information security policy

Policy objectives

1. This policy is intended to establish the necessary policies, procedures and an organisational structure that will protect Countrywide Tax & Trust Corporation Ltd's (referred to as CTTC Ltd) information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met.

2. Compliance with this policy is necessary to ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents.

Scope

This policy applies to:

3. This policy is intended to establish the necessary policies, procedures and an organisational structure that will protect CTTC Ltd's information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met.

4. Compliance with this policy is necessary to ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents.

4.1. All Directors and the information processed by those Directors.

4.2. All employees of CTTC Ltd, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by CTTC Ltd but engaged to work with or who have access to company information, (e.g. computer maintenance contractors) and in respect of any externally hosted computer systems

4.3. All CTTC Ltd operations run out of the offices in Warwickshire.

4.4. The Policy applies to all locations from which CTTC Ltd's systems are accessed (including home use).

4.5. All information processed by CTTC Ltd in pursuit of all its operational activities, regardless of whether it is processed electronically or in paper form.

4.6. All information transferred or exchanged with third parties, or held by third parties on behalf of the CTTC Ltd, regardless of whether it is processed electronically or in paper form.

Communication

5. This policy will be made available to all those working for or on behalf of CTTC Ltd and made available on the CTTC Ltd website.

Policy Statement

6. It is the policy of CTTC Ltd to ensure that:

   6.1. Information assets and information processing facilities shall be protected against unauthorised access

   6.2. Information shall be protected from unauthorised disclosure

   6.3. Confidentiality of information assets shall be a high priority

   6.4. Integrity of information shall be maintained.

   6.5. Business continuity plans shall be produced, maintained and tested.

7. All breaches of information security, actual or suspected, shall be reported and investigated in line with CTTC Ltd's policies.

8. Controls shall be commensurate with the risks faced by CTTC Ltd.

Information security objectives

9. The objectives of the Information security management system are:

10. To provide the necessary policies, procedures and an organisational structure that will protect CTTC Ltd's information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met.

11. To ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents.

12. To preserve the appropriate level of confidentiality, integrity and availability of CTTC Ltd's information assets and critical activities.

Responsibilities

13. CTTC Ltd's Directors shall be accountable for ensuring that appropriate and effective information security controls are implemented, monitored and reviewed.

14. CTTC Ltd's Directors shall be responsible for ensuring that the CTTC Ltd's information security objectives are aligned with the organisation's objectives.

15. CTTC Ltd's Directors shall ensure continuous compliance. Compliance will be a matter for periodic review by the Directors.

16. The Directors are responsible for setting the priorities for the information security work programme. A programme of reviews and assessments of security effectiveness will form part of this programme, and will establish an agenda for security improvements.

17. The role and responsibility for facilitating information security at an operational level shall be determined by the Directors who will instruct senior staff members or third parties to carry out their instructions as appropriate.

18. CTTC Ltd's Directors are responsible for implementing security policies and procedures including with the third parties that they manage. As part of the formal assessment of security effectiveness, they will:

    - Consider data protection issues as part of the design and implementation of systems, services, products and business practices;
    - Make data protection an essential component of the core functionality of the processing systems and services
    - Anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals
    - Only process the personal data that is needed for the businesses' purpose(s) and only use the data required for those purposes

19. Core privacy considerations are incorporated into existing project management and risk management methodologies and policies to ensure:

    - Potential problems are identified at an early stage
    - Increased awareness of privacy and data protection
    - Legal obligations are met and data breaches are minimised
    - Actions are less likely to be privacy intrusive and have a negative impact on individuals

    These considerations include:

    - Data Breaches and Information Security Incidents
    - Access control
    - Security of equipment
    - Payment Card Industry Compliance (PCI)
    - Security and storage of information
    - Sharing and disclosing information
    - Retention and disposal of information

- Vacating premises or disposing of equipment
- Systems development
- Network security
- Cyber security
- Access control to secure areas
- Data Back up
- Software
- Use of removable media

20. All staff whether permanent or temporary are responsible for the protection of CTTC Ltd's information assets, enabling the confidentiality, integrity and availability of these assets to be maintained.

21. All third party suppliers to the CTTC Ltd are to conform to this policy.

22. All staff must adhere to all policies relating to Information Security. Non- compliance will be subject to investigation and may result in disciplinary action under CTTC Ltd's disciplinary procedure. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation and may include, but not be limited to:

- Loss of access privileges to information assets or information processing facilities
- Disciplinary action including termination of employment and legal prosecution
- Other actions as deemed appropriate by, the Human Resources and the Directors and legal advice.

Governance

23. Information Security will be governed and the effectiveness measured by the following methods:

- Internal audit
- External audit, e.g. third party penetration testing to ensure that an independent company has examined CTTC Ltd's security, and adhere to the Payment Card Industry Standard (PCI DSS).
- Business continuity and service continuity exercises
- Management review e.g. risk assessments, results of awareness training, lessons learnt from security incidents and identified improvement opportunities.

24. The results from these processes will enable the business to review the effectiveness of the controls and continually develop the Management System.

25. The Directors will review and approve the prioritisation of information security aspects of the

internal audit schedule on an annual basis, ensuring that every business process is audited at least once in a 3 year period.

26. The Information Security policy will be reviewed every 12 months or when there are significant changes to ensure it is being implemented correctly and consistently and that quality is maintained.

Security awareness and training

27. Staff with access to information assets and information processing facilities shall be educated on their information security responsibilities. Education shall be provided as part of the induction process so that new staff completely understand their responsibilities in the protection of information assets and information processing facilities.

28. Staff shall be provided with on-going security education and supporting reference materials. The Directors shall provide refresher courses and other security related materials to regularly remind staff about their obligations with respect to information security.

29. The security responsibilities of third parties shall be made clear at an early stage of the contract by the person responsible for engaging the third party.

Risk Management

30. A systematic approach to information security risk management has been adopted to identify business needs regarding information security requirements (including legal, contractual and regulatory) and to create an effective operational information security framework.

31. Information security risk management is not a one-off exercise with a single set of control recommendations which remain static in time but a continual process.

32. The implementation of the information risk strategy shall be based on formal methods for risk assessment, risk management and risk acceptance and independent of technology or software.

Cyber Security

33. CTTC Ltd has a disaster recovery and business continuity plan in place. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but CTTC Ltd employs a range of tools and good practice to minimise the risk to its information and systems including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Passwords

- Removable Media
- Sharing and disclosing information
- Cloud storage systems
- Viruses
- Equipment, media and data disposal

34. CTTC Ltd employs a range of technology and processes to help it achieve a good security platform. These range from up to date firewalls and core networking equipment, through antivirus controls and a secure wireless configuration, to encrypted devices, two factor authentication and mobile device management.

Information Risk Management Regime

35. The Directors manages information risk proactively and provides information to staff and members about information retention and disposal and information sharing. The team works with service areas to help them design and implement regimes for their information.

Secure Configuration

36. CTTC Ltd's IT service providers has default build processes for corporate devices and ensures that operating systems, services and applications are patched against known vulnerabilities. There is an inventory of all corporate computers and servers. Servers and network environments log activities for auditing purposes.

Network Security

37. The IT service providers ensures network security; this is periodically reviewed to ensure they meet security and business needs.

Managing User Privileges

38. The IT service providers manages core systems and applications. User logins for computers are managed by the IT service providers and access to information must be approved by the Directors and permissions granted in line with job requirements. Wherever possible user activity is logged, access to activity logs is restricted to IT Administrators and Internal Audit.

User Education and Awareness

39. The Directors periodically send emails and information about threats to the organisation.

Incident Management

40. CTTC Ltd has processes and recovery places for disaster recovery and business continuity. These are managed by the Directors and IT service providers. There are also processes in place for the

reporting and response for information and security incidents.

Malware prevention

41. The IT service providers manages CTTC Ltd's antivirus and malware solutions. Signatures for malware and antivirus are updated automatically on all company computers.

Monitoring

42. The IT service providers logs all system and security events across its server environment, and has software in place to alert for internal and external threat attempts.

Removable Media Controls

43. The IT service providers has implemented a solution to manage USB devices on company devices.

Home and Mobile working

44. The IT service providers employs a number of tools to ensure security of information for home and mobile working, including Mobile Device Management solutions to encrypt corporate mobile devices and corporate information on personal devices. Additionally the council uses two factor authentication.

Continual improvement

45. The Directors shall ensure continual improvement of the information security management system.

Legislation and standards

46. The list below contains some of the legislative and regulatory requirements CTTC Ltd must comply with:

- Data Protection Act 2018
- General Data Protection Regulation
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- Companies Act 2006 Health & Safety at work Act
- Employment Legislation
- Bribery Act 2010
- Fraud Act 2006
- The Payment Card Industry Data Security Standard

Countrywide
TAX AND TRUST CORPORATION LTD

Glossary

Asset	Anything of value to the organisation. There are many types assets including information, software, hardware and intangib assets such as reputation.
Availability	The property of being accessible and usable upon demand by a authorise entity.
Business continuity management	A process that identifies potential threats to an organisation ar the impacts to operations that those threats, if realised, migl cause. It provides a framework for building the capability for a effective response that safeguards the interests of its ke stakeholders and the organisation's reputation.
Confidentiality	The property that information is not made available, or disclose to unauthorised individuals, entities or processes.
Information security	Information security is the protection of information from a wic range of threats in order to minimise business risk. Informatic security is the preservation of confidentiality, integrity, ar availability of information.
Information security management system	Part of the overall management system, based on a business ris approach, to establish, implement, operate, monitor, revie maintain and improve the organisation's information security.
Integrity	The property of protecting the accuracy and completeness assets.
Physical security	This covers the assets, and the way those assets are used, t restrict physical access and the presence of people in certa locations to stop theft of, or damage to, assets and property. Th may include locked doors and movement controls.

This document was last updated in April 2019.