Company Information Security Policy

Version No: 1.06
Issue Date: March 2018

Version : Company Information Security Policy – 1.06
Created : 17th April 2012
Updated : 24th March 2017

Company Dynamics Software

272 Bath Street • Glasgow • G2 4JR
Tel: 0333 370 1570 • Fax: 0141 280 2888 • Email: info@companydynamics.co.uk

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Owner's Name
V1.00	17 Apr 2012	New Document	Stuart R Hunt
V1.01	30 Mar 2013	Annual Review	Stuart R Hunt
V1.02	05 Feb 2014	N3 Acceptance Review	Stuart R Hunt
V1.03	05 Jan 2015	Address change	Stuart R Hunt
V1.04	25 Feb 2016	Annual Review	Stuart R Hunt
V1.05	27 Feb 2017	Annual Review	Stuart R Hunt
V1.06	24 Mar 2018	Annual Review + GDPR Compliance	Stuart R Hunt

For more information on the status of this document, please contact:	Stuart R Hunt Technical Director Company Dynamics Software 272 Bath Street Glasgow G2 4JR Tel No: 0333 370 1570 E-mail: stuart.hunt@companydynamics.co.uk Internet: www.companydynamics.co.uk
Date of Issue	April 2012
Reference	Information Security Policy
Company Registration	CD Support Ltd. (SC374884)

Policy Title:	Company Information Security		
Issue Date:	17th April 2012	Review by date:	31st March 2019
Version:	V1.06	Issued by:	Stuart R Hunt
Aim:	Set a level of governance of data management, transmission and Storage		
Scope:	Outline company procedures and expected handling of data management and reporting policies		
Associated Documentation:	**Legal Framework:** The Data Protection Act (1998), Copyright Designs & Patents Act (1988), Computer Misuse Act (1990), Human Rights Act (1998), EU GDPR (2018) **Policies:** Email Discipline and Usage		
Review Process:	Annually from review date above.		
Responsible for Implementation:	Stuart R Hunt – Technical Director		

1. Introduction

This top-level information security policy is a key component of Company Dynamics overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

2. Objectives, Aim and Scope

2.1. Objectives

The objectives of Company Dynamics Information Security Policy are to preserve:

- **Confidentiality** – Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** – Information shall be available and delivered to the right person, at the time when it is required.

2.1. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Company Dynamics by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.

3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Company Dynamics or supplied under contract to it.

4. Responsibilities for Information Security

4.1. Ultimate responsibility for information security rests with the Technical Director of Company Dynamics and shall be responsible for managing and implementing the policy and related procedures.

4.2. Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

4.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

4.4. The Information Security Policy shall be maintained, reviewed and updated by the Technical Director. This review shall take place annually, sooner on new directives.

4.5. Managers shall be individually responsible for the security of their physical environments where information is processed or stored and oversee subordinates.

4.6. Each member of staff shall be responsible for the operational security of the information systems they use.

4.7. Each system user shall comply with the security requirements that are currently in force and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

4.8. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

5. Legislation

Company Dynamics is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Company Dynamics, who may be held personally accountable for any breaches of information security for which they may be held responsible. Company Dynamics shall comply with the following legislation and other legislation as appropriate:

- The EU General Data Protection Regulation (2018)
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

6. Policy Framework

6.1. Management of Security

- Responsibility for Information Security shall reside with the Technical Director
- Company Dynamics Technical Director shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

6.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

6.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

6.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

6.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

6.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

6.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

6.8. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.9. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

6.10. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Technical Director.

6.11. Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of Company Dynamics's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

6.12. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Technical Director. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

6.13. Classification of Sensitive Information

Company Dynamics shall implement the appropriate information classifications controls, based upon the results of formal risk assessment and technical overview to secure any information assets.

The classification "Company Confidential" – shall be used for client records and client details shared with other client approved companies. In order to safeguard confidentiality, the term "Company Confidential" shall not be used on correspondence to the client. Documents so marked shall be held securely at all times in a locked room to which only authorised persons have access. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Documents marked "Company Confidential" not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.

The classification “Company Restricted” - shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals.
- Make it more difficult to maintain the operational effectiveness of the organisation.
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations.
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity.
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies.
- Breach statutory restrictions on disclosure of information.
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.
- Company Restricted documents should also be stored in lockable cabinets

6.14. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation’s property without permission from the Technical Director. Users breaching this requirement may be subject to disciplinary action.

6.15. User media

Removable media of all types that contain software or data from external sources or that have been used on external equipment. Require the approval of Technical Director before they may be used on Company Dynamics systems. Such media must also be fully virus checked before being used on the organisation’s equipment.

Users breaching this requirement may be subject to disciplinary action.

6.16. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of company security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

6.17. Accreditation of Information Systems

Company Dynamics shall ensure that all new information systems, applications and networks include a security plan and are approved by the Technical Director before they commence operation.

Policy Progression - System Level Security Policies (SLSPs) for systems should be developed for each system in order to distinguish between the security management considerations and requirements of each. In this way, specific responsibilities may be assigned and obligations communicated directly to those who use the system.

6.18. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Technical Director.

6.19. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Technical Director. Users shall not install software on the organisation's property without permission from the Technical Director. Users breaching this requirement may be subject to disciplinary action.

6.20. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

6.21. Reporting

Managers shall keep the Technical Director informed of the information security status of the organisation by means of regular reports and reviews.

6.22. Policy Audit

This policy shall be subject to audit by the Technical Director.

6.23. Further Information

Further information and advice on this policy can be obtained from Stuart R Hunt -- Technical Director, 0333 370 1570.

7. Policy approved by:

Signature:  Date: 24/04/18

Stuart R Hunt – Technical Director – Company Dynamics – CD Support Ltd.