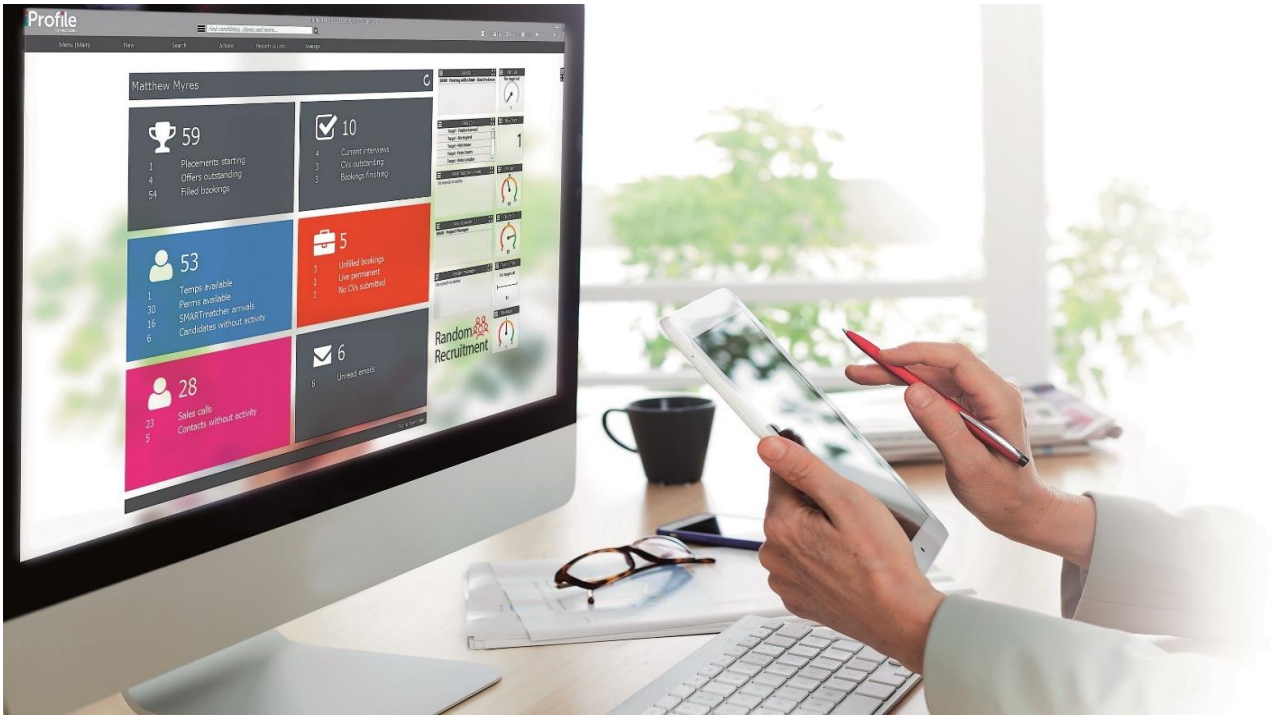
INFORMATION SECURITY AND DATA PROTECTION POLICY

Policy for the Information Security Management System employed to keep our own and our clients' information secure



Author	Linda Clark
Document Title	Information Security and Data Protection Policy
Date Last Updated	16/11/2017 17:02
Date of Next Review	
Document Path	M:\Microdec\HR\Policies and Procedures\Information-Security-and-Data-Protection-Policy.docx
Pages	10
Copyright	Unauthorised publication or distribution is prohibited. All Right Reserved Copyright Microdec © 2017
Security Classification	Public

Revisions Table

Version	Reviewed by	Date	Sections Changed?
1.00		16/11/2017	First Draft

Table of Contents

1. Introduction

The Information Security and Data Protection Policy sets out how Microdec and its delivery partners/suppliers manage and provide security to Microdec Plc and its clients' sensitive information within the boundaries of developing recruitment agency software and the processing and hosting of personal information on behalf of our clients.

It explains the responsibilities that various functions, roles and individuals have for ensuring the confidentiality, integrity (accuracy) and availability of information within our organisation.

Microdec fully supports and complies with the principles of the General Data Protection Regulation (GDPR) which are summarised below:

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 'storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Having an information security policy is government and industry best practice. It helps to prevent any events, accidental or malicious which results in the unauthorised access or disclosure of electronic files, paper documents and online services.

The security policy and its compliance is mandatory for all members of staff employed by Microdec Plc. It will also be a minimum compliance for contractors undertaking work for and on behalf of Microdec.

Client data stored in "Microdec's Cloud" is physically stored in a UK-based ISO 27001 and ISO 14001 certified data centre, operated by Rackspace® therefore any aspect relating to the physical location (i.e. security and utilities) of this Data Centre will not form part of the scope.

The Microdec Board is committed to maintaining and developing an information systems infrastructure, which has an appropriate level of security and data protection.

The Microdec Board of Directors has made a commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the information systems management. Our commitment includes activities such as ensuring that the proper resources are available to work on these systems and that all employees affected have the proper training, awareness, and competency.

Because the needs of our business change, we recognise that our management system must be continually changed and improved to meet our needs. To this effect, we aim to continually review and update our objectives and processes.

2. Purpose and Scope

The purpose of this policy is:

- To bring to the attention of all staff the need to improve and maintain security of information systems, and to advise managers of the approach being adopted to achieve the appropriate level of security.
- To bring to the attention of all managers and staff, their responsibilities under the requirements of relevant legislation, including Data Protection and Human Rights legislation and guidance, and the importance of ensuring the confidentiality of personal and sensitive data.
- To ensure that the company complies with current legislation and EU Directives, meets its statutory obligations and observes standards of good practice.
- To minimise the risk of security breach and prosecution.
- To ensure business continuity plans are established, maintained, and tested.
- To ensure all personnel are trained on information security and are informed that compliance with the policy is mandatory.
- To ensure all breaches of information security and suspected weaknesses are reported and investigated.

This policy applies to:

- All aspects of cyber and information security, including the specification, design, development, installation, operation, connection, use and decommissioning of the systems, services and equipment used to store, process, transmit or receive information.
- All Microdec data, and any data that Microdec is processing for other data controllers.
- All Microdec employees - who should understand their responsibilities in using the company's information assets including its systems.
- Microdec staff engaged in designing and implementing new technology solutions, who must reflect the policy requirements into their design and build.
- Contracted suppliers that handle/access/process data. Contracted suppliers must provide the security measures and safeguards appropriate to the nature and use of the information. All Contracted suppliers of services to Microdec must comply, and be able to demonstrate compliance, with the company's relevant policies and standards.

3. Accountabilities

The Information Security Officer is the accountable owner of the Information Security and Data Protection Policy and is responsible for its maintenance and review in-conjunction with the Data Protection Officer.

Any exception to the Information Security and Data Protection Policy must be risk assessed and agreed by the Information Security Officer.

Delegation of responsibilities is outlined in detail in the Information Security Management Procedures.

4. Policy Statements

4.1. Responsibilities

All Employees must:

- only access systems and information, including reports and paper documents to which they are authorised and for the purposes of carrying out their function in the company.
- use systems and information only for the purposes for which they have been authorised.
- familiarise themselves with this Policy, and all applicable supporting policies, procedures, standards and guidelines. Compliance with this Policy is mandatory, and any employee failing to comply may be subject to disciplinary procedures.
- comply with all appropriate legislation and all corporate policies, standards, procedures and guidelines.
- not disclose confidential information to anyone without the permission of the manager of the team(s) who are the information owners or to comply with a statutory duty.
- keep their passwords secret, and not allow anyone else to use their account to gain access to any system or information.
- notify their manager, or the Information Security Officer of any actual or suspected breach of Information Security, or of any perceived weakness in Microdec's security policies, procedures and practices or infrastructure.
- ensure that where they are responsible for the management of third parties, the third parties are contractually obliged to comply with this Policy and that those third parties are aware that their failure to comply may lead to contract termination.
- not use non-Microdec email accounts (i.e., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct Microdec business, thereby ensuring that company business is never confused with personal business and data is always traceable within the corporate systems.

Senior Leadership Team (SLT) and Managers must:

- Ensure that their staff are fully conversant with this Policy and all associated policies, standards, procedures, guidelines and relevant legislation, and are aware of the consequences of non-compliance.
- Develop compliant procedures, processes and practices for use in their business areas.
- Notify the Information Security Officer of any suspected or actual breaches or perceived weaknesses of information security.
- Notify the Data Protection Officer of any suspected or actual data protection breaches
- Take appropriate disciplinary action in the event of misconduct, and non-compliance with security or data protection policies.
- Ensure recruits are trustworthy and appropriate employment checks have been carried out.

4.2. Legislation

All employees will comply with all current legislation. Laws relating to information security and data protection including those outlined below:

Data Protection Act 1998 and GDPR

At the heart of the GDPR is the concept that EU citizens will have a clearly defined set of rights regarding the use of their personal data. Personal information relating to identifiable individuals must be kept accurate and up to date. It must be fairly obtained and securely stored. Personal information may only be disclosed to people who are authorised to use it.

Copyright. Patents and Designs Act 1988

Documentation must be used strictly in accordance with current applicable copyright legislation, and software must be used in accordance with the licence restrictions. Unauthorised copies of documents or software may not be made under any circumstances.

Computer Misuse Act 1990

This Act addresses the following offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.

Part 3 of The Employee Practices Code

Provides best practice guidance on monitoring of emails, phone calls and internet access in the context of the Data Protection Act.

EU Directive on Privacy and Electronic Communications (PECR)

Defines legal standards for the processing of personal data, and the protection of privacy in the electronic communications sector.

Human Rights Act 1998

Based on the European Convention on Human Rights.

4.3. Physical Access

Security for software or electronic information will be largely secured by central controls and through information owners. However additional physical security systems are required to (a) protect the electronic systems and (b) protect manual or other forms of information media (such as tapes).

Centrally controlled screen savers will be switched on and must not be overwritten. Passwords must not be shared.

The use of memory sticks or downloading to CD's is controlled and is generally not permitted. It is only permissible where it is essential for the business and only by the Technical Services or Infrastructure Teams.

All staff must adhere to the physical building security, the office must not be left insecure when unattended. All documents should be stored based on their confidentiality rating and desks should be clear.

4.4. Escalation

If an exposure to a breach of security or data protection is identified, all staff must follow the Data Breach Notification and the Information Security Incident Logging policies. The exposure must be reported to the Information Security Officer, Data Protection Officer or a member of the Senior Leadership Team who will decide:

- The best course of action to take.
- Those individuals who need to know about the exposure.
- If the breach is likely to result in a risk to the rights and freedoms of individuals and so for example if left could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation, then the exposure will be reported to the individual(s) affected and the relevant supervisory authority.

4.5. Risk Assessment

Each team is responsible for reporting security or data breaches. The associated risk assessment will be carried out by the Information Security Officer and/or Data Protection Officer. They must assess the risk of unauthorised access to information, software, and hardware and consider the risk in relation to each information technology resource and establish security controls and protection in relation to that risk. Risk must be assessed in relation to the following factors:

- Quality of the control mechanism
- Size of the threat
- Potential loss.

4.6. Business Continuity

Microdec PLC are fully committed to our employees and clients and recognise the potential strategic, operational and financial risks associated with a business interruption and the importance of maintaining our services if an emergency occurred.

A Business Continuity Plan is in place which assesses the impact of the cause of the interruption to services and ultimately calls on a Disaster Recovery Plan to re-establish working systems.

4.7. Related Policies

Information Classification policy

Access Control policy

Acceptable Use policy

Data Breach Notification policy

Password policy

Client Data Storage policy

Receipt of Data policy

Information Retention and Disposal policy

Remote Access policy

Mobile Device Security policy

Firewall policy

Remote Working policy

Information Security Incident Logging Policy.

Head office, UK
Jupiter House
Warley Hill Business Park
The Drive, Brentwood
Essex CM13 3BE
•
+44(0) 1277 227778

Sydney, Australia
Level 34, AMP Centre
50 Bridge Street
Sydney
NSW, 2000
•
+61(2) 8216 0772

Manchester, UK
Stafford Court
145 Washway Road
Sale, Cheshire
M33 7PE
•
+44(0) 161 8711044