Document Issue			
Date	Version	Approver	Title
08.08.2017	1.2	Phil Miller	Managing director

Introduction

Information, in whatever form it takes, is a valuable asset to the company and consequently needs to be suitably protected. Protecting information is not only a corporate responsibility; it is also a responsibility which all staff working for ABCA Systems Ltd. must take seriously.

Objective of this Policy

The objective of this policy is to ensure that all paper and electronic records containing person identifiable information, or any other confidential/sensitive information (including corporate or commercially sensitive information) is suitably secured when not in use and is not left visible on an unattended desk.

This policy applies in particular to working areas, such as desks or tables, which should not have confidential, sensitive, commercially sensitive or person-identifiable information left on them whilst unattended for an extended period.

The objective of this policy is also to ensure that ABCA Systems Ltd. adheres to the obligations placed upon it by the Data Protection Act.

What is a Clear Desk Policy?

A clear desk policy directs all of us to clear our desks at the end of each work day. This not only includes documents and notes, but also post-it notes, businesses cards, and removable media (CDs, floppy disks, memory sticks). Following a clear desk policy will help us reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible in plain view.

The Benefits of a Clear Desk Policy

Compliance; a clear desk policy is not only ISO 27001/17799 compliant, it also complies with basic privacy principles. The Data Protection Act requires companies in the UK to ensure that personal information is kept secure.

Discourage dishonesty; employees usually leave sensitive information on their desk. Paper notes are usually the worst culprit, containing names, phone numbers, and even user names and passwords visible in plain view. These habits encourage dishonest employees, cleaners, and maintenance staff to view information they should not have access to.

Reduce Stress; *when* staff are organised they can spend more time concentrating on work rather than becoming stressed because they're unable to provide something which is asked of them in a reasonable time frame.

Resources and costs; a clear desk policy will encourage employees to use digital versions of documents, significantly reducing costs of paper, ink toner, and printer maintenance.

Good impression; unannounced visits are made to ABCA offices and a clean and tidy workspace can assist with any impressions formed about ABCA.

What you need to do?

Personal Mobile phones should be kept away at all times (including lunch breaks). If you need to use your phone you must be in a secure location, such as the canteen area, or outside.

Your computer should be locked whenever you leave your seat, and all customer details should be cleared from the screen.

Coats, bags and other personal effects should be kept in the appropriate place, and lockers are provided.

Remove printing and photo copying from printers as soon as printing is finished.

Key Principles

The key principles of adhering to the Clear/Secure Desk / Clean Screen Policy are:

- To reduce the risk of a security breach or information theft;
- To reduce the risk of confidential or sensitive information / documentation being stolen or accessed by unauthorised individuals which could damage the integrity of ABCA Systems Ltd;
- To help demonstrate compliance with the Data Protection Act 1998;
- To create a culture of staff responsibility in relation to the handling and care of personal data and other confidential information;

Definitions

*Personal Data***:** this is information which can identify a living individual – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name, private address, home telephone number, National Insurance number etc.

*Sensitive personal data***:** this is where the personal data contains details such as the following which relates to an individual:

- Physical or mental health condition
- Ethnic origin
- Religious beliefs
- Sexual orientation
- Political views
- Criminal convictions

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

*Corporately and commercially sensitive information***:** this information may, through improper disclosure, cause reduced competitiveness or breach procurement practices.

Scope

This policy applies to all permanent, temporary or contracted staff employed by ABCA Systems Ltd. who can access information independently or under supervision.

The policy applies to desks, tables, computer screens, photocopier, fax and printer areas.

Responsibilities

- All employees and contractors are required to comply with the Secure Desk Policy.
- Line managers are responsible for monitoring compliance and providing guidance to staff on the implementation of the policy.
- All employees, elected members, contractors and agency staff have a responsibility to report security incidents and breaches of this policy as quickly as possible via the Council's Incident Reporting Procedure.

ABCA Systems Ltd. will take appropriate measures to remedy any breach of the Policy through the relevant framework in place. In the case of an employee, then the matter may be dealt with under the disciplinary process. Internal

reviews by management and Internal Audit, including spot checks will take place in order to identify potential breaches of this policy.

Secure desk procedure - PROTECTING INFORMATION

Confidential or sensitive information, whether held electronically or on paper records and other valuable resources should be secured appropriately when staff are absent from their workplace and at the end of each working day. To facilitate this, the following guiding principles have been produced which cover both non-electronic (e.g. manual/paper files) as well as electronic forms of information. In addition, reference is made to the display of information on the computer / laptop screen as well as to the security of personal property.

- Desks must be cleared at the end of each working day of any confidential or person identifiable information. Files containing confidential information must be locked securely in desks, filing cabinets or designated secure rooms at all times, other than when being used by staff. All efforts must be made to keep this information secure and not readily accessible to non-authorised staff.

- To reduce the risk of a breach of confidentiality and adherence to the Data Protection Act, when disposing of person identifiable information, ensure that it is destroyed securely using approved methods of waste disposal.

- Health & Safety – desks and other work spaces should be sufficiently tidy at the end of each working day to permit the authority's cleaning staff to perform their duties.

Electronic Storage Devices

For the purposes of this policy, electronic data and equipment will not be treated differently from manual records and equipment if they contain the same type of confidential, sensitive and/or personal information. Computing and all other equipment containing data will therefore be treated with the same level of security as paper based resources.

- To ensure the security of information held electronically, lock away portable computing devices such as Laptops or PDA devices when not in use and where appropriate.

- To ensure the security of information held on mass storage devices such as CDROM, DVDs or USB drives, lock these away in a secure drawer at the end of the working day

- USB drives and other such items must be locked away even if they are encrypted.

Personal Computers, laptops and Personal Digital Assistants (PDA's)

Computers and laptops must not be left logged on when unattended. When staff have to leave their desks for any reason, they must lock the computer by using the 'Control, Alt, Del' keys simultaneously or by pressing the 'Windows' key and the letter 'L'. Access to the computer/laptop must be protected by passwords.

As far as practicable, when sensitive or confidential information is being worked on, the window must be closed or minimised, or the computer locked when unauthorised persons are in close proximity to the screen.

If sensitive or confidential information is visible to an unauthorised person standing in close proximity to computer/laptop screen, they could be asked to move away to protect the confidentiality of this information.

Printers, Photocopiers and Fax Machines

To avoid accidentally printing to an unintended network device, computer users should additionally check that their default printer is correct before printing any documents.

Where documents are scanned using photocopiers or multi-functional devices, ensure that scanned documents are correctly rooted to the 'owner' of the document and then accurately filed to a secure network drive.

Personal data must be cleared from printers, photocopiers and fax machines immediately on completion. If these are no longer required, the items must be shredded or sent for secure disposal.

It is the responsibility of the person who sends information to be printed, to ensure they collect their documents. If information is of a confidential/sensitive nature and it is misplaced or missing, this should be logged as an incident to your line manager.

Training Implications

To be informed of Clear Desk/ Clear Desk / Secure Desk policy as part of induction.

Review / Monitoring Arrangements

All staff are responsible for monitoring their compliance with the principles / procedures detailed in this policy; departmental managers and supervisors should also monitor compliance on a regular basis. This policy will be continually monitored and will be subject to a regular review which will take place one year from the date of issue and at three year intervals thereafter. An earlier review may be warranted if one of the following occurs:

- As a result of regulatory / statutory changes or developments;
- Due to the results/effects of critical incidents;
- For any other relevant or compelling reason.

Non-Conformance

There is a requirement for all staff to comply with this policy, and where requested, to demonstrate such compliance. Failure to comply will be regarded as a disciplinary incident, and will be dealt with under the appropriate Human Resource policy.