DEK Technologies Employee ICT Policy and Procedure

Abstract

This document describes the Information and Communications Technology (ICT) and Information Security (IS) policies and processes within DEK Technologies as they relate to employees.

The information within is provided as a guide to all employees of DEK Technologies (DEK Corporation Pty Ltd [Australia], DEK Technologies Sweden AB [Sweden], DEK Technologies Vietnam Co LTD [Vietnam], and DEK Italia SRL [Italy]), hereafter referred to as the Company or as DEK.

Local site addendums and deviations from this policy can be found in the ICT section of the Quality Management System.

Contents

1 ICT POLICIES

1.1 PHYSICAL SECURITY

1.1.1 Building Access

External access to offices of the Company is via an authorized access control mechanism. This is controlled by local Administrators.

Buildings that belong to or are rented by the Company shall be manually alarmed during periods of no occupancy.

1.1.2 Server and Telecommunications Rooms

Server and telecommunications rooms shall be kept locked when not occupied. Access to the rooms, and equipment held within is by authorized persons only, or with constant supervision by authorized persons.

Server and telecommunications rooms must be kept clear of flammable materials and any other unnecessary equipment, furniture, boxes, etc for fire safety reasons

For names, see chapter “Authorized persons” in the site-specific documents mentioned in 1.1.

1.1.3 Client machines

Individuals are responsible for security of the client machines allocated to them, particularly with respect to Laptops taken outside the secure office environment.

Client machines which at any time are at risk of grab and run theft must be locked away out of view or otherwise secured physically with an adequate locking mechanism (eg. Kensington lock).

1.1.4 Clear Desk Policy

A clear desk policy is enforced to protect Customer Information and Assets. Employees must ensure no customer Intellectual Property (IP) is left on desks when unattended for extended periods (including overnight). It must be secured in desk drawers.

1.2 USER ACCESS AND DATA SECURITY

The Company has a complicated security situation due to our close coupling with one of our main clients. The presence of this Client’s network introduces a second potential conduit for external attack. This increases the need for strict internal security. We cannot rely purely on our external firewalls to protect us from intruders.

1.2.1 Networks

DEK segregates the data networks based on client requirements.

- Internal DEK voice and data network (provided via both Ethernet cable and wireless).
- A client specific network reached via a router, which is controlled by the client (provided via Ethernet cable only for safety reasons).

It is possible to reach the Company network from an external source via a VPN connection.

1.2.2 Availability of computer facilities

Computer facilities shall only be available to users for approved purposes.

Users shall use computer facilities in an effective, efficient, and lawful manner.

"Computer facilities" includes computer hardware, computer software, all other computer equipment and data in digital form owned, leased, provided or used under licence by the Company and all cables and other equipment necessary for the networking of the Company's computers; computer facilities owned or maintained by other persons, but available for use through an agreement with the Company; online services hosted or carriage services provided by the Company including internet, intranet and e-mail services; and all other computing services wherever situated where access is by means of computer facilities referred to in previous paragraphs of this definition.

Only formally approved computer facilities (i.e. currently the DEK country sites) may be connected to the Company's networks.

No computer facilities may be connected to customer network access points or to customer network equipment that resides on the Company premises. If computer facilities should be connected to such network or network equipment in the course of business activities related to a customer, then local ICT Administrator should be contacted.

1.2.3 User access

A computer user shall obtain a computer account prior to the user's initial use of any computer facilities.

User shall use computer facilities within the limits of the access privileges granted to the computer user and in compliance with any Restricted Access System developed or used by the Company.

1.2.4 Use of computer facilities

1.2.4.1 General

User shall not use any other person's computer account despite any permission from the account holder unless it is a special group account authorised by the 'Authority' (See section 4)

User shall not attempt to discover or use any other computer user's secret identifier or to circumvent any Company's restricted access system;

User shall not use any computer facilities which the computer user is not authorised to use;

User shall not reproduce, decompile, reverse engineer, disclose or transfer any computer software provided by the Company without the written permission of the 'Authority' (See section 4);

User shall not use computer facilities in violation of the terms of any software licence agreement;

User shall not use computer facilities to infringe any intellectual property rights or to contravene any intellectual property laws;

User shall not without the permission of the owner, or of the 'Authority' (See section 4), copy, rename, change, examine or delete files or content belonging to another computer user or a third party;

User shall not without the permission of the 'Authority' (See section 4) copy, rename, change, examine or delete files or content belonging to or controlled by the Company;

User shall not attempt to modify computer facilities, obtain extra resources without authorisation, or degrade the performance of any system or attempt to subvert the restrictions associated with any computer system, computer account, network service or computer software protection;

User shall not tamper or attempt to tamper with any filtering software installed by the Company on any computer facilities for the screening of prohibited content;

User shall not use terminals, computer equipment, network devices or any other associated equipment in an unauthorised or unlawful manner;

User shall not use any networks or computing facilities at other sites connected to Company owned networks in an unauthorised or unlawful manner;

'Authority' (See section 4) shall determine what an authorised manner is for the purposes of previous two sections.

User shall not collect, remove or discard any computer output without the owner's permission;

User shall not use site computer facilities for the purpose of private profit making or other private commercial activities.

1.2.4.2 Conduct online

User shall not use computer facilities to transmit, distribute or make available online any internal e-mail communication or other materials prepared for use within the Company to persons external to the Company unless expressly authorised by the Company Management and/or 'Authority' (See section 4).

User shall not use computer facilities to make an unauthorised disclosure of any confidential information of the Company.

User shall not use computer facilities to harass or interfere with the work of other users.

User shall not use computer facilities to misrepresent himself or herself as another person online.

User shall not use computer facilities to create, download, store, transmit, distribute, publish, display or make available on-line content which is defamatory; constitutes sexual harassment; constitutes sexual discrimination; constitutes racial discrimination; is prohibited content, unless in compliance with any restrictions imposed by the law regulating such content; commit any act prohibited by law or in breach of the Company internet code of practice, any of the Company regulations or the Company procedures and policies;

User shall not use computer facilities to reproduce, download, transmit, distribute, publish or make available online any computer software or other copyright material unless authorised by law or with the express permission of the copyright owner and in compliance with the terms of any applicable copyright licence or notice, and shall ensure that the terms of any applicable copyright licence or notice are communicated to any person to whom the copyright material is transmitted, distributed, published or made available.

1.2.4.3 Use of e-mail

User shall use e-mail services provided by the Company only in accordance with this regulation.

a) User shall not use e-mail services provided by the Company to send unsolicited commercial e-mail; or send defamatory, obscene, abusive, fraudulent, intimidatory harassing or repetitive messages or attachments; or engage in sexual harassment or any other conduct prohibited by law.

b) User shall not access or attempt to access the electronic mailbox of another e-mail user.

c) The Company email addresses are provided solely for use in the Company's business. The Company email system must not be used to transmit personal material, in particular any material which may be considered offensive or defamatory. Staff are encouraged to establish personal email addresses.

d) The Company email addresses must not be used to subscribe to non-business-related services, in particular social networking (e.g. Facebook) or other free internet services.

e) Email should be regarded in the same way as conventional written correspondence and must therefore conform to company policy in terms of tone and content.

f) Email should only be used for transmission of work-related information, confidential information, in particular any commercial in confidence or sensitive material relating to the Company or a third party, where appropriately must be marked 'Commercial-in-Confidence', 'Confidential' or similar.

g) Emails that contain anything that is defamatory or offensive must not be sent. Defamatory messages may expose both the Company and the sender of the message to legal liability. Senders of offensive emails, including pornography, may be liable under laws relating to censorship and under the criminal law. This includes forwarding emails that are sent to you by third parties.

h) Respect the privacy of others. Do not send any personal information regarding any person via email without their consent. This may breach the provisions of the law regulating privacy policy.

i) Do not send any emails which may be considered harassing or menacing, even as a joke. This is also prohibited under the criminal law.

j) Do not send any email that contains materials that may be considered discriminatory (even if you think that it is funny, you never know where your message may end up). Discriminatory material is anything that focuses upon a person's age, gender, marital status, sexual preference, race, political beliefs or any physical or mental impairment.

k) Email correspondence is part of the business records of the Company and therefore should be stored and managed in an appropriate manner.

l) Some of our clients requires the use of email SSL encryption. Forwarding Company emails outside of the Company network (e.g. to private email accounts) is a direct breach of this requirement, and is therefore not allowed.

m) Do not use email for any purposes relating to chain letters and limit the use of "All Staff" or other group alias email to appropriate purposes.

n) Inform your local ICT of any virus alert, who will circulate the alert, if appropriate.

1.2.4.4 Virus Protection

All computers running Microsoft Windows are to have antiviral software installed and operational at all times. This software shall be kept current.

1.2.4.5 Web Access

The Company relies upon the discretion of its staff to make appropriate use of access to the Internet while using the Company network. Staff should ensure that they comply with any laws (including those

relating to harassment) and other guidelines published by the Company from time to time. In particular, the network may not be used to access pornography and other offensive material. Downloading and display of such material is prohibited.

1.2.4.6 Standards of Conduct

Each Company staff member is responsible for any misuse of the IT and Telephony resources made available to them by the Company, with specific reference to: -

a) Company supplied ICT resources should not be used for harassment or similar inappropriate behavior;
b) Company supplied ICT resources should not be used for accessing sexually explicit, offensive, or erotic material;
c) Company staff should be aware that copyright rules may apply to information found on the Internet. Approval for the use and distribution of such information must be obtained from the owner/author;
d) Company supplied ICT resources should not be used for the purposes of probing or illegal hacking;
e) The use of non-business related “streaming” and downloading of audio, video and software (including Internet radio, YouTube, video news feed, etc.) should be avoided;
f) Check with local ICT site administrator or ict@dektech.com.au if required to download large programs for business purposes. These may already be available locally. If not, an off-peak download should be scheduled;
g) Company supplied ICT resources should not be used for any type of illegal activity;
h) The use of pirated software or data is strictly prohibited; and
i) Company staff should not knowingly distribute viruses or bypass any installed virus detection system in place

1.2.5 Client network security

Client security rules are governed by the Client and regulated in separate agreements between DEK and its Clients. Hard copies of these agreement are filed and accessible via the Management team.

1.2.6 Protection of client information

Client Information shall be handled as Confidential Information.

Client Information will not be excessively stored, printed, copied, disclosed or processed by other means outside the purpose for use.

Client Information is processed and stored logically separated from DEK internal Information and from that of other clients.

Upon conclusion or termination of DEK’s work for a client, client information will be sanitised and securely destroyed, including all working copies, backups and archival copies, in any electronic or non-electronic form.

1.2.7 Connection of hardware to networking or computer facilities

No computer hardware may be connected to the Company networks except with the prior approval of the ‘Authority’ (See section 4).

1.2.8 Test equipment on networks

The nature of the Company's business requires some test equipment be connected to our networks. It is often not practical, or even possible, to follow the strict user account regime detailed above. Test equipment may have common users and published root passwords as warranted.

These machines may not contain sensitive data. They may not be configured to access core servers with non-password authentication. They may not be used except for test functions. In particular web browsing, file storage. The ICT Administrator must be notified of their connection to the networks and provided with the root password or equivalent.

1.2.9 Insecure Work Practices and Tools

Tools and practices which are deemed by the industry to be insecure must be avoided for safer alternatives. Examples include:

- use of rlogin/rcp/ftp permits password sniffing, and should be replaced with ssh/scp/sftp
- rather than opening of X11 server to access from any client (xhost +), ssh X11 tunneling should be used.

Sharing of folders or drives of the computer facilities should be avoided except if explicitly allowed by the 'Authority'

Where appropriate, the ICT Administrator shall disable support for such unsafe features.

1.2.10 Right to monitor

The Company reserves the right, subject to compliance with privacy laws, to examine all computer files and electronic mailboxes of individual users and to monitor all computer usage for the purpose of ensuring compliance with applicable laws, Company regulations, Company internet code of practice and Company procedures and policies and to maintain a secure and effective computing environment

1.2.11 Third Party Equipment and Software

All software purchases must be made with the involvement of the ICT Site Administrator. User may install open-source and freeware software on their workstations and server home directories provided care is taken not to introduce malicious software and that all licence conditions are adhered to.

1.2.12 Home directory/Disk encryption

BitLocker must be enabled on all compatible Windows laptops/desktops. On Linux laptops/desktops encryptfs must be used.

1.2.13 Physical Data Security

Use of USB memory sticks permitted for temporary transfer of IP, provide files are wiped afterwards. Permitted for storage of non commercial-in-confidence material.

Use of external hard disks is permitted so long as they are suitably encrypted or secured in a locked cabinet.

Printouts should not be left lying about.

1.2.14 Use of Non-DEK Computer Equipment

Use of personally owner computers for any DEK or customer sensitive information is not permitted due to data security risks. Connection of personally owned computers on customer networks is strictly prohibited.

1.2.15 Isolation of DEK/customer networks

There shall be no bridging between these two distinct networks.

1.2.16 Removal of Project Files at Completion of Project

When an employee completes a project for customer all customer IP is to be removed from that employee's laptop. Permanent data should be stored on appropriate servers only.

1.2.17 Legality

The Company shall comply with all licence conditions of all software packages used. This includes use of open source code and shareware. In particular, evaluation copies and non-commercial use provisions.

The Company shall comply with both the letter and the spirit of the licences. Use of non-commercial licences and long-term use of evaluation licences is prohibited.

1.3 PASSWORD MANAGEMENT

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of personal information and business data as well as the Company entire networks. As such, all employees (including contractors, vendors and third parties with access to the Company systems) are responsible for taking the appropriate steps to select and secure their passwords.

Any users that violate password security may be subject to breach of conduct clause.

1.3.1 Login identities

All users shall be required to authenticate themselves (login) to gain access to an information system.

All users shall identify themselves uniquely before being authenticated to a system.

1.3.2 Remote access

Remote access to the Company network via VPN (Virtual Private Network) shall only be provided to staff on an as-needed basis, upon request from their manager.

Staff working on any computer connected to the Company network via VPN shall observe all policies detailed in this document, the same as if they were physically connected to the Company network at the office.

VPN access must NOT be installed on any publicly accessible PCs.

1.3.3 Password Strength

Blank passwords for any login identity shall not be used.

Passwords shall be a minimum of eight characters.

Passwords shall contain characters from at least three of the following four categories: uppercase alphabet characters (A–Z), lowercase alphabet characters (a–z), Arabic numerals (0–9) and non-alphanumeric characters (for example, !$#,%).

Passwords must not be based on the user's account name and common or dictionary terms must be avoided.

Passwords used for DEK accounts must not match those used for employee's non-DEK accounts.

1.3.4 Regular password changes

Users are responsible for regularly changing passwords (at least every 90 days) for their own computer equipment and externally accessible systems. These are: - Computer Equipment (For example: desktops or laptops)

For the Email and VPN access, the 'Authority' (See section 4) shall establish password expiry periods of not more than 90 days. The same password shall not be reused for at least 12 cycles.

For local administrated computer equipment (like desktops or laptops) the user must update the password every 90 day. The same password shall not be reused for at least 12 cycles.

For some of our clients they themselves have implemented password expiry systems that force password change every 90 days, with pending expiry notified to the user by email.

Users shall change newly allocated passwords upon first login independent of system requirements to do so.

1.3.5 Password confidentiality

All PCs must be password protected.

Passwords must not be shared, written or recorded in plain text on automated logon scripts or hard coded into software, revealed to others in any manner or recorded on any medium unless that medium is stored and secured in a restricted area. All users must treat passwords as private and highly confidential.

Compromised accounts or passwords must be reported to the Authority and/or action taken to change passwords whenever a loss of confidentiality is suspected.

No PCs may be left with unsecured logins at the office outside normal working hours.

Where possible, all PC systems shall be configured to disallow 'remembering' and display of the last User ID at the point of login.

Only ICT approved password managers (such as KeePass) may be used. Web based systems (such as LastPass) may not.

1.3.6 Intruder lockout

All PCs shall be configured to automatically lock after 15 minutes without user input. Password or biometric authentication shall be required to unlock the workstation.

1.4 DOCUMENT HANDLING

The procedure to classify and store documents related to the Company's activities or to Company's relations with customers is regulated by the "Documented Information" procedure, DEK-18:0183, or equivalent local office adaptations.

1.5 BACKUP AND REVISION CONTROL

Don't use external services (such as GitHub, Google Drive or DropBox)

Don't use memory sticks/external drives unless encrypted.

1.5.1 Physical File Transfer

In some situations, transferring files between systems is best achieved using a USB memory stick. In such situations the files should be wiped with a tool such as shred. (merely deleting the file can leave recoverable data behind)

1.6 BREACH OF REGULATION

The 'Authority' (See section 4) may immediately and without notice upon discovery of a suspected breach of this regulation suspend user's access to computer facilities; isolate and, if necessary for the purposes of investigating the suspected breach, impound any item of computer equipment, whether belonging to the Company or not, which the Authority suspects has been or is being used in breach of this regulation.

Where the 'Authority' (See section 4), after initial investigation, is satisfied that no breach of this regulation can be substantiated; or a breach of this regulation has occurred, but that any such breach is a minor one, the 'Authority' (See section 4) shall terminate the suspension.

Where the Authority after initial investigation determines that a breach of this regulation may have occurred, the Authority shall refer the matter to the Company Director(s) to be dealt with in accordance with the applicable industrial Award or Agreement, or where no Award or Agreement applies, as determined by the Director(s).

1.6.1 Reporting Obligation of Employees

All employees are obliged to report breaches of security, breaches of privacy and breaches of policy to ICT or company management. DEK has a corresponding obligation to ensure the employee is not penalised for the report.

2 ICT PROCEDURES FOR USERS

2.1 NEW EQUIPMENT

2.1.1 Justifying

The effort in justifying ICT infrastructure expenditure is proportional to the cost involved (purchase, installation, maintenance, etc.) and the overall impact on operations.

2.1.2 Purchasing

Refer to each sites Quality Manual for information regarding purchasing.

An ICT Site Administrator must be notified before any ICT related purchases are made, no matter how small the value.

2.2 DECOMMISSIONING EQUIPMENT

Once a laptop, desktop, server or anything with a hard drive is to be decommissioned the data on the hard drive has to be permanently erased.

There are two methods for doing this:

a. Erased the data with a method called purge;
b. Physically destruct the hard drive.

This action must be performed by DEK ICT Administrators.

2.3 NEW USERS

A laptop or desktop (as appropriate) is purchased by the Company Site Core Management and passed on to the ICT Site Administrator for initial installation and set-up.

Accounts are established as per the New Starter Checklist, or as instructed by the Company Site Core Management.

As part of the induction process, new starters are given a run-down on the various ICT systems and facilities.

2.4 USER ACCOUNTS

Client user accounts are ordered by the General Manager or ICT Administrators.

Internal Company accounts are managed by the ICT Administrators.

2.5 HELP AND SUPPORT

Business critical faults must be addressed by seeking out (in person or via phone) one of the ICT Administrators for urgent attention to the problem.

Access outside of normal working hours is not guaranteed.

Less urgent matters are to be addressed via email to ict@dektech.com.au.

Security incidents, issues, faults or any other questions related to security are to be addressed via email, via phone or in person to local IS personnel.

2.6 VIRUS/FIREWALL PROTECTION

Only ICT approved virus/firewall software shall be used on client machines.

For virus/firewall software approved for use on client machines see chapter “Virus/Firewall Protection” in the site-specific documents mentioned in 1.1.

All components of this software must be operational at all times.

2.7 KEEPING THE SOFTWARE UP TO DATE ON EQUIPMENT

Each user that has been given computer equipment has the responsibility to keep that equipment updated with the latest patches for the following software on that equipment:

a. Operating system
b. Anti-Virus software
c. Security patches for any software on the equipment

Within 72-hours from that an update or patch has been publish, the user must have updated the equipment with that patch.

The easiest way for the user to comply with this is to allow automatic updates for the operating system, anti-virus software and other software.

3 AUTHORITIES

For the purpose of preceding text the is defined as persons belonging to the management and/or ICT or IS groups. For more detailed specification of Authority see site specific documents.

3.1 DECISION MAKING

The responsibility for decision making in technical aspects and day to day running of the ICT infrastructure is delegated to the local ICT Administrators.

Where financial, customer or policy impacts are involved; the local Company Management must be consulted.

Any decisions related to or involving security aspects must be taken with involvement of IS personnel.

3.2 IMPLEMENTATION

The local Core Management team is responsible to ensure that intent of these policies and procedures is followed.

The local ICT Administrators have responsibility and Authority to implement all aspects of these policies.

Local Information Security personnel have responsibility and Authority to participate in the implementation of these policies, review, change and amend the policies.

From time to time, other Company personnel will be assigned responsibly and authority for implementing aspects of these policies, under direction from ICT Administrators.

4 AUDIT

To ensure that the policies and procedures are followed by each employee of DEK, half-year internal audits will be performed by each site's General Manager or an auditor appointed by the General Manager.

The user audit will follow the Audit Checklist that is kept and updated by the DEK IS/IT group.

5 REVISION INFORMATION

Rev A	2009-03-05	New doc number allocated. Document re-written to include DEK-Vn needs
Rev A (Se)	2012-05-18	Local version created to suit DEK-Se needs after external IT audit in Sweden, and then which became the official global version.
Rev B	2019-03-19	Transferred to new template format. Made more universal for all DEK sites. Strengthened to be more in line with client requests and ISO27001. Removed Terminology section

This document replaces DEK-05:0111, which was written when DEK consisted of Australia only.

Rev A	2006-07-24	First issue of the document
Rev B	2006-01-03	Revamped due to CAR-007 and CAR-008 * ACCESS added to heading of chapter 3, and whole chapter re-written * Minor corrections to chapter 4 due to DEK persons being overseas * Chapters 5, 6.1 and 6.2 are new.
Rev C	2007-02-19	Added section about disposition of electronic records. Fixed table of contents
Rev D	2007-09-13	Removed implementation details. These can be found in the ICT Wiki.
Rev E	2008-06-16	* Title changed to include 'Policy' and 'ICT' * Added Information Repositories and Applications to section 1. * Printers also added. * Policy around handling guests is added. Sec 2.4 * Sec 2.3.4, According to a clients Information Access Agreement, it is not necessary to physically separate the DEK and clients networks. This clause is removed. * Sec 2.5, aspects of password security and backup changed * Expanded on implementation details in a Procedures section, including help facilities. * Authorities section moved to bottom and completed. * Terminology section added.