

# Company Policies

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION</b>	<b>2</b>
<b>2</b>	<b>RESPONSIBILITIES AND AUTHORITIES</b>	<b>2</b>
<b>2.1</b>	<b>2.1. Standards</b>	<b>2</b>
<b>3</b>	<b>IS/IT POLICY COMPANY POLICIES</b>	<b>2</b>
<b>3.1</b>	<b>Policy for using IT equipment, Internet and e-mail</b>	<b>2</b>
3.1.1	Scope	3
3.1.2	Rules	3
3.1.3	General	3
<b>3.2</b>	<b>Safety rules</b>	<b>3</b>
3.2.1	Payments	3
3.2.2	Downloading program files, games, music, etc.	3
3.2.3	Backup	4
3.2.4	3.2.4 Connection of equipment not belonging to CDEng	4
3.2.5	Internet at home	4
3.2.6	Private use of the Internet and e-mail	4
3.2.7	Monitoring and monitoring of policy	4
<b>3.3</b>	<b>Email policy</b>	<b>5</b>
3.3.1	Purpose	5
3.3.2	Scope	5
3.3.3	Responsible/Manager	5
3.3.4	Procedure	5
3.3.5	Email	5
3.3.6	Some short guidelines for email	5
3.3.7	Private email	6
3.3.8	Monitoring and follow-up of policy	6
<b>4</b>	<b>DOCUMENT CONTROL</b>	<b>6</b>

## 1 Introduction

The purpose of this document is to establish and document the Company's various Policies, and details which document in the Quality Management System that contains each such policy.

## 2 Responsibilities and Authorities

The President of the Company is responsible for the Company policies.

- It can be updated by the President, or by a member of the board of the company.
- Following the procedure – everyone working for the Company, as employee of hired in, shall follow the Policies defined in this document.
- Deciding what to do if necessary to deviate from the procedure – if anyone working for the Company finds himself/herself in conflict with a Policy or in a situation not covered by these Policy, they shall inform their closest manager for guidance and/or escalation to the Company's President (or a member of the Board).

### 2.1 2.1. Standards

We are using ISO 9001

## 3 IS/IT Policy Company Policies

### 3.1 Policy for using IT equipment, Internet and e-mail

All IT equipment in the form of hardware and software and use of this, including the Internet and e-mail, have become part of our everyday lives. This new technology has given and continues to give us unmatched opportunities to communicate as well as search and retrieve information. In business terms, the company sees this as useful and exciting. The company supports, and encourages all employees to continue developing with regards to the use of IT equipment and new technologies.

CDEng owns all IT equipment as well as all information in the IT systems, such information generated or otherwise processed in or regarding the service. At the same time, private use of the company's equipment and systems is accepted to a limited extent and under certain conditions. This policy aims to clarify the rules governing the use of Internet and e-mail services. By setting these guidelines for our IT usage and making these known in the organization, employee's integrity is also protected as anyone can act based on the prerequisites.

Everyone must be aware that there are risks considering when using IT, both ethical and security-related. When we use the Internet at the workplace, we act as representatives of the company because electronic communications leave track with the company's name. It is therefore important that your use of the company's IT resources does not violate the CDEng values and business goals. The traces you leave for you must in no way create bad will or adversely affect the Group's operations.

If you are unsure about the application of the policy, you should first contact your nearest boss. Questions of ethical nature are also answered by the Human Resources Manager and Security-related Issues of IS / IT Manager.

### 3.1.1 Scope

This policy covers all employees at CDEng and all employees of the company (consultants, interns, graduates, etc.).

### 3.1.2 Rules

For all Internet usage and all electronic communications that occur through company computers and user identities, the following general, ethical and security rules apply.

### 3.1.3 General

It is only allowed to participate in discussion groups on web pages related to the company's business and your business within the company, with the close of the boss's consent.

It is absolutely forbidden to download and search information (visit, chat and surf) on web pages that are related to material that violates Swedish law. The following email usage is forbidden:

- Distribution of chain letters.
- To send / search SPAM (bulk mail) and various unsolicited commercials.
- Participating in mailing lists that are not consistent with the company's business goals and values.
- Sending e-mails that may be offensive to the recipient. Ethical rules It is absolutely forbidden to participate in discussion groups as well as retrieve and search information (visit, chat and surf) on websites that are related to:
  - Pornography.
  - Discriminatory content related to gender, sexual orientation, disability, ethnicity, religion or other beliefs.
  - Other offensive or otherwise inappropriate sites and use the Internet for illegal, offensive or unethical purposes.

In all communications on the Internet, the use can be registered and traced to the company. CDEng does not want to be linked to the above-mentioned activities, so breach of the above rules is regarded as a breach of contract.

## 3.2 Safety rules

### 3.2.1 Payments

No transactions may be performed on the Internet where the company's credit card number or the like must be entered unless special routine with special security login is established.

### 3.2.2 Downloading program files, games, music, etc.

Our PC is a tool and therefore the local environment must be as close to the original configuration as possible. Download of executable files, such as Program files downloaded from the Internet are prohibited. If there is a need for such download, contact the company's IT department.

It is also not permitted to download games, music or the like that are unrelated to the company's business.

### 3.2.3 Backup

The IT department is responsible for backup capture on file servers while the user is responsible for backing up the contents of local hard disks.

### 3.2.4 3.2.4 Connection of equipment not belonging to CDEng

External equipment that is not part of CDEng may not be connected to the network due to virus-risk and non-updated software. If there is a special need for connection, the equipment must first be checked by the IT department.

### 3.2.5 Internet at home

For security reasons, relatives and friends may not use the company's network for their Internet connection. The ID and password of a system belonging to CDEng is the employee's personal and may not be disclosed to another person, either inside or outside the company. If the company's equipment (not Home-PC) is used with private Internet subscriptions, the company's policy must be followed.

### 3.2.6 Private use of the Internet and e-mail

Internet services and e-mail are provided by the company to enable employees to effectively manage their duties and be able to communicate, retrieve and save work-related information. Private use is also accepted for non-work-related communications if you do not violate the content of this policy. This use must be done sparsely and with good judgment, which means that use should primarily take place outside of working hours and that it is not allowed to charge a computer / hard drive with private material of a larger amount. The company's file servers may not be used to store private information at all. The company accepts no responsibility for private information. For monitoring and follow-up of the policy, the same principles apply to the private use as for the work-related.

### 3.2.7 Monitoring and monitoring of policy

Internet usage monitoring is conducted to ensure that usage follows our policy. It is not about controlling employees without protecting the company's information. This information is one of the company's most important assets and a significant competitive factor. The company also owns computers as well as all information in the computers and is thus legally responsible for the content and must therefore be able to make controls. Therefore, the company may not be excluded from this content by encryption or the like. Users' activities on the Internet are logged by the IT department. The log contains information about which websites were visited, by whom, as well as the time and date. If the log shows that any unauthorized visit of unauthorized websites, this information will be forwarded to the responsible manager and HR manager. The IT department also makes regular checks on the content of the company's so-called File servers. The IT department has equipment and the opportunity to read the employee's e-mail but should read the user's consent before reading the e-mail. In exceptional cases, the IT department may read the e-mail after approval by the nearest manager and staff manager. In such cases, a union representative will be notified. This applies to the following situations:

- Danger of information security.
- Suspicion of crime.
- Unfair behavior which is the basis for termination or damages.

Failure to comply with current policy / rules be a breach of the employment contract and in serious cases lead to termination.

### 3.3 Email policy

#### 3.3.1 Purpose

To facilitate the use of email as a work tool.

#### 3.3.2 Scope

All employees within CDEng as well as company-appointed staff (consultants, interns, graduates, etc.).

#### 3.3.3 Responsible/Manager

HR Manager

#### 3.3.4 Procedure

In all external communications where we use the company's resources, we also act as representatives of CDEng. It is therefore important to respect CDEng by acting in accordance with the values of the group and that the communication you perform and the possible traces you leave behind do not in any way adversely affect the Company. Questions about this are usually answered by the Personal Manager. Ethical rules for all internet usage and all electronic communications that occur through company computers and user identities, the following ethical rules apply.

#### 3.3.5 Email

Email is part of our internal and external service communications, improper use can cause misunderstandings, conflicts and stress, so accuracy in handling is important. Choose which way is the most effective, sometimes it's better to call, or send text. Most get too many e-mails that do not concern them. It takes time to open and watch, since you cannot determine if it is important or not. This creates stress and it can also cause you to miss the important mail. If more people are the addressee of an e-mail, it is also unclear who is expected to act, which may cause more time for the same or no-one.

#### 3.3.6 Some short guidelines for email

- Do not send email e-mail to anyone in an email group. Think about who really needs the information and send only to them.
- Address the person (s) you want to act on your message, and put the others as real need information about the case in the line below = CC i.e. copy to. Never send a copy to anyone about you not sure that this needs this information.
- Describe your case as well as possible deadline short but clearly in the subject heading.
- Use only "Urgent Flag" if something is very important and requires direct treatment.
- Enter auto signature that clearly tells who is the sender, i.e. name, company name, telephone number, fire promise, etc. An email will not end with just "Greetings Nisse".
- An e-mail is an important document as a regular letter. Write briefly but so to the reader

understands what is meant. Use a protected language without unnecessary abbreviations, use spell check.

- An e-mail message is sometimes forwarded or answered to other addressees, so be sure to describe the case so that even third parties understand what is meant / desired to be performed. This becomes particularly important in cases where a legal conflict can be fought.
- Forward only in case of emergency and nothing that you have not processed.
- When answering an email, delete any attachments, "answer without attachment", and consider whether to answer all "reply to all" or only the sender "reply".
- Preferably, you prefer a message by email.
- For shared opinions about how to solve a thing, handle etc., break the mail exchange and use the phone.
- Insert "Out of office message" with clear information about when you return to the case when you are not accessible and can reply to email.

### 3.3.7 Private email

It is allowed to use the company's computers for private use to a limited extent. The private use of the company's resources must not be such as to cause capacity problems and thus additional costs for the company. For private use, the company's ethical rules must always be followed.

The following are not allowed:

- Distribution of chain letters.
- Sending SPAM, unwanted commercials.
- Participating in mailing lists that are not consistent with the company's business goals and values.
- Sending e-mails that may be offensive to the recipient.

**Private use of e-mail should always be sparse and with good judgment.**

### 3.3.8 Monitoring and follow-up of policy

Note that both computers and all information in the computer are the company's property. The company is legally responsible for the content and therefore may not be excluded from this by encryption or the like. The IT department has the equipment and the ability to read the employee's e-mail, which does not happen normally. However, exceptions constitute the following situations:

- Danger of information security
- Suspicion of crime
- Unfair behavior that is reasonable grounds for termination or damages

## 4 Document control

This document shall undergo annual management review by the President together with the Board of Directors.

This procedure, and all its changes, shall be communicated to all employees and hired personnel:

- on recruitment
- be readily available through our IT system for all employees and hired personnel