

ELECTRONIC COMMUNICATIONS ACCEPTABLE USE POLICY

Version:

Date:

Authorised by:

Owner:

Contacts:

Change Requests:

HOW TO READ THIS DOCUMENT

This policy contains best-practice decisions with respect to user access to your company's information.

The document contains the following:

- *Purpose of the policy*
- *Scope of the policy*
- *Considerations pertaining to security awareness, incident reporting and user non-compliance*
- *A glossary of terms used within the document*
- *The actual policy decisions or objectives that your organisation should make with respect to security.*

The policy decisions are presented in a graded manner. The first option of each decision is classified as high security, the second as medium security and the third as minimum security. It is up to management to decide which of the three options is most appropriate to implement as a final policy. It is advisable that you consider the impact of each decision before making a final choice. Consider the following:

- *Financial implications related to implementing the specific policy decision*
- *Potential software or hardware requirements*
- *Staff capabilities and capacity*
- *The importance (criticality) of the information assets the policy is meant to protect.*

In addition, for each policy decision the target audience has been identified, as follows:



This indicates that the decision is directed at all users in the organisation



This indicates that the decision is directed at management.



This indicates that the decision is directed at IT administrative staff.

Table of Contents

1	POLICY PURPOSE.....	1
2	POLICY SCOPE.....	2
3	ROLES & RESPONSIBILITIES.....	3
4	POLICY DECISIONS.....	4
4.1	IDENTIFICATION & AUTHENTICATION.....	4
4.2	AUTHORISATION & ACCESS CONTROL.....	6
4.3	SECURE INFORMATION EXCHANGE.....	12
4.4	INFORMATION INTEGRITY & RECOVERABILITY.....	13
4.5	NON-REPUDIATION.....	16
4.6	AUDITABILITY.....	17
5	AWARENESS & EDUCATION COMMITMENTS.....	18
6	INCIDENT REPORTING.....	18
7	CONSEQUENCES OF NON-COMPLIANCE.....	18
8	RELATED DOCUMENTATION.....	18
9	GLOSSARY OF TERMS.....	19

1 POLICY PURPOSE

Electronic Communications facilities such as telephone, fax, Internet and e-mail are useful business tools as they represent a quick, cost effective and easy way to communicate vital business information to partners, customers and suppliers. These characteristics, though advantageous, introduce a variety of risks into our environment. Some of these risks are:

-
.....
.....
.....
-
.....
.....
.....
-
.....
.....
.....

The aim of this Acceptable Use Policy is to allow our employees to exploit the business benefits of services such as telephone, fax, Internet or e-mail in a secure and legally correct manner.

The objectives of this policy are:

-
.....
.....;
-
.....
.....;
-
.....
.....

2 POLICY SCOPE

For the purpose of this policy, acceptable use of electronic communications services is defined as:

The terms and conditions under which access to our company's telephone, fax, Internet, e-mail and other related services is granted to users and the rules of conduct governing user behaviour with respect to such services.

The table below lays out the scope of Electronic Communications adopted in this policy:

<i>Type of Use</i>	<i>Considered subject to the Electronic Communications – Acceptable Use Policy</i>	<i>Comments</i>
Internal communication to colleagues, co-workers or management via fax, e-mail, FTP or through the Intranet web site.	YES	It is important to maintain good “netiquette” when communicating internally, as inappropriate behaviour, even unintentional, may result in damage to the company's reputation, system overloads or legal liabilities.
Public communication with another organisation, via fax, e-mail, FTP or to their Internet web site.	YES	This is particularly important in the light of recent legislation on Electronic Communications and Transactions. Poorly phrased or inappropriate communications could result in legal obligations harmful to our organisation.
Public communication with any third party (irrespective of whether this is for business purposes or not) via fax, e-mail, FTP or to their Internet web site.	YES	Whenever individuals make use of company provided Fax, Internet or Email services, they represent not only themselves but also the company. It is for this reason that the code of conduct outlined in this policy applies to all communications, whether business related or not.
Communications with any third party via Internet Newsgroups or bulletin boards.	YES	This mode of communication is even more dangerous than email as anyone who connects to a news service or bulletin board may read the messages posted there. This is why it is important that individuals realise that they do not only represent their own views but by association also the views of our company.
Voice communications via company telephone services.	YES	The telephone services provided by the company are a form of electronic communications and fall under the scope of this policy.

3 ROLES & RESPONSIBILITIES

<i>Function/Role*</i>	<i>Description</i>	<i>Accountability or Responsibility</i>
Users	Anyone who uses our electronic communications services. This includes employees, employees of our business partners, contractors, consultants, temporary workers etc.	All users are responsible for complying with this and related policies and standards for security.
The Information Security Steering Group (or equivalent).	A high-level group responsible for coordinating information security issues across the organisation.	The Information Security Steering Group is responsible for the formulation of company policy and standards for security, ensure that risks are identified and managed, resolve disputes and endorse any proposed non-compliance with this and related policies.
Information Security Manager	The individual with corporate-wide responsibility for coordinating information security.	The Information Security Manager is responsible for the provision of specialist support and advice to the Information Security Steering Group, plan and coordinate information security related activities in the organisation and undertake independent monitoring of security status in accordance with this and related policies.
Information Owners	The designated person that is responsible for the security of a set of information. The owner determines the level of access control to the information within the parameters of our company policies.	Information Owners are responsible for determining the security requirements of their systems, authorising access and defining access privileges in accordance with sound risk management principles and the directives of the Information Security Steering Group.
Security Administrators	The individual who is responsible for configuring and updating workstations, servers, networks, firewalls and other IT equipment used in support of company business activities.	Security Administrators must ensure that security controls are implemented in accordance with Information Owner directives and this and related policies.
Internal Audit	The group or individual who is responsible for providing the Board of Directors and top management with objective reports on the effectiveness of internal controls, the accuracy of records, the reliability of information, and the safeguarding of assets.	Internal Audit is responsible for monitoring compliance to this and related policies.

The roles and responsibilities for information security defined here should be a summary of the detailed roles and responsibilities of all relevant stakeholders in your organisation. Provided here are the most common roles associated with security management and should be modified to reflect your company's unique security organisation

4 POLICY DECISIONS

4.1 Identification & Authentication

4.1.1 User identification and authentication



To ensure that individuals remain accountable for their actions,

→ DEGREE OF CONTROL →	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
8.7.3 Electronic commerce security		
8.7.4 Security of electronic mail		
8.7.5 Security of electronic office systems		
8.7.7 Other forms of information exchange		
9.1.1 Access control policy		

4.1.2 Impersonation



To ensure that unscrupulous individuals do not abuse our Electronic Communications facilities by claiming to be someone that they are not, and therefore exceeding their authority,

→ DEGREE OF CONTROL →	Hi	<p>.....</p> <p>.....</p> <p>.....</p>
	Med	<p>.....</p> <p>.....</p> <p>.....</p>
	Min	<p>.....</p> <p>.....</p> <p>.....</p>

Related ISO/IEC 17799 Controls

- 8.7.3** Electronic commerce security
- 8.7.4** Security of electronic mail
- 8.7.5** Security of electronic office systems
- 8.7.7** Other forms of information exchange
- 9.1.1** Access control policy

4.2 Authorisation & Access Control

4.2.1 User Access Authorisation



To maintain effective control over access to our Electronic Communications Services,

↑ DEGREE OF CONTROL ↑	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
9.1.1	Access control policy	
9.2.1	User registration	
12.1.5	Prevention of misuse of information processing facilities	

4.2.2 Personal Use



Our Electronic Communications facilities are provided by the company for employees to conduct company business. Therefore,

→DEGREE OF CONTROL→	Hi	<p>.....</p> <p>.....</p> <p>.....</p>
	Med	<p>.....</p> <p>.....</p> <p>.....</p>
	Min	<p>.....</p> <p>.....</p> <p>.....</p>

Related ISO/IEC 17799 Controls

- 8.7.4 Security of electronic mail
- 8.7.5 Security of electronic office systems
- 8.7.7 Other forms of information exchange
- 9.1.1 Access control policy
- 12.1.5 Prevention of misuse of information processing facilities

4.2.3 Unacceptable Use



In order to protect our company from any liability due to the misuse and abuse of our Electronic Communications facilities,

↑ DEGREE OF CONTROL ↑	Hi
	Med
	Min

Related ISO/IEC 17799 Controls

- 8.7.4 Security of electronic mail
- 8.7.5 Security of electronic office systems
- 8.7.7 Other forms of information exchange
- 12.1.5 Prevention of misuse of information processing facilities

4.2.4 Establishing modem connections



Uncontrolled modem connections provide an instant extension to our internal network over insecure public lines and may expose our company to unauthorised access by hackers. For this reason,

→ DEGREE OF CONTROL →	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
8.7.5 Security of electronic office systems		

4.2.5 Personal web servers



Many recent attacks aimed at damaging company information and systems have been carried out by exploiting weaknesses on personal web servers established by employees on their company workstations or laptops. For this reason,

→ DEGREE OF CONTROL →	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
8.7.3 Electronic commerce security		

4.2.6 Third Party Users



In order to manage the exposure that our organisation may face (e.g. legal liabilities, public embarrassment etc.) as a consequence of improper use of our Electronic Communications facilities by third parties,

↑ DEGREE OF CONTROL ↓	Hi
	Med
	Min
<p>Related ISO/IEC 17799 Controls</p> <p>8.7.4 Security of electronic mail</p> <p>8.7.5 Security of electronic office systems</p> <p>8.7.7 Other forms of information exchange</p> <p>9.1.1 Access control policy</p> <p>12.1.5 Prevention of misuse of information processing facilities</p>		

4.3 Secure Information Exchange

4.3.1 No default protection

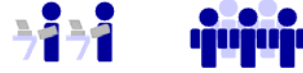


Employees are reminded that our company’s electronic communications facilities (whether e-mail, Internet, voice or fax) are not automatically protected against disclosure to unauthorised individuals. Therefore,

→ DEGREE OF CONTROL →	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
8.7.4 Security of electronic mail		
8.7.5 Security of electronic office systems		
8.7.7 Other forms of information exchange		
10.3.2 Encryption		
10.3.3 Digital signatures		

4.4 Information Integrity & Recoverability

4.4.1 Receiving e-mail (see also Paragraph 4.2.3)



The receipt, failure to detect or the introduction of a virus embedded in an e-mail message can not only damage the recipient’s computer and data but can also spread throughout our company network, wreaking havoc. Therefore,

→ DEGREE OF CONTROL →	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
8.3.1 Controls against malicious software		

4.4.2 Junk e-mail (Spam) (see also *Paragraph 4.2.3*)



Spam (the electronic equivalent of junk mail), may cause our company’s e-mail systems to overload and affect the availability of the service. Therefore,

↑ DEGREE OF CONTROL ↓	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
8.7.4 Security of electronic mail		

4.4.3 Downloading program software, files or information from the Internet (see also Paragraph 4.2.3)



Because the Internet is generally considered an unreliable source of information and due to the risks associated with downloading large and/or virus infected files and programs as well as due to the potential legal liabilities associated with the use of unlicensed software downloaded from the Internet

→ DEGREE OF CONTROL →	Hi	<p>.....</p> <p>.....</p> <p>.....</p>
	Med	<p>.....</p> <p>.....</p> <p>.....</p>
	Min	<p>.....</p> <p>.....</p> <p>.....</p>
<p>Related ISO/IEC 17799 Controls</p> <p>8.3.1 Controls against malicious software</p> <p>12.1.2 Intellectual property rights</p> <p>12.1.5 Prevention of misuse of information processing facilities</p>		

4.5 Non-Repudiation

4.5.1 User Responsibility



Because the safe use of our Electronic Communications Facilities is dependent on the discipline of individual users, with respect to keeping their personal passwords, tokens or PINs safe and on the termination of open sessions and logging out of the electronic communications facilities when any such systems are left unattended,

→ DEGREE OF CONTROL →	Hi
	Med
	Min
Related ISO/IEC 17799 Controls		
6.1.1 Including security in job responsibilities		

4.6 Auditability

4.6.1 Expectations of Privacy



While our company respects the individual’s right to privacy as that right is guaranteed under the EU Data Privacy Directive, in the context of electronic communications facilities, which are provided for the company’s operational needs, certain restrictions are unavoidable. Consequently,

→ DEGREE OF CONTROL →	Hi
	Med
	Min

Related ISO/IEC 17799 Controls

- 9.7.2 Monitoring system use
- 12.1.1 Identification of applicable legislation
- 12.1.4 Data protection and privacy of personal information
- 12.1.7 Collection of evidence
- 12.2.1 Compliance with security policy
- 12.3.1 System audit controls

5 AWARENESS & EDUCATION COMMITMENTS

The cooperation of every single individual making use of our Electronic Communications Facilities is essential for the effective management of security within our organisation.

To raise the awareness of important security issues in our organisation and to assist all users in performing their duties in a secure way,

- Employees must be provided with relevant awareness tools to enhance awareness and educate them regarding the range of information security threats and the appropriate safeguards.
- Individual training must be provided with any technical training being appropriate to the responsibilities of the user's job function. In particular, training on good password management practices is mandatory for all users.

6 INCIDENT REPORTING

Individuals who desire to report instances of violations of this policy, or who discover or know of an unauthorised or attempted intrusion, or wish to suggest improvements, are encouraged to contact one of the individuals below:

- <Insert contact details here>, Tel. +49 (xx) xxxx-xxx
- <Insert contact details here>, Tel. +49 (xx) xxxx-xxx

7 CONSEQUENCES OF NON-COMPLIANCE

Intentional violations of this policy may be grounds for denial of access privileges or disciplinary action in line with our company's code <insert link here>.

8 RELATED DOCUMENTATION

The following documents are referenced in this document:

- Logon Policy;
- Access Authorisation Form;
- Modem Use Authorisation Form
- Web Server Authorisation Form
- End-User Procedures for the Use of Encryption Technologies.

9 GLOSSARY OF TERMS

<i>Terms used</i>	<i>Definition</i>
Access Controls	Rules and mechanisms that which control access to Information Systems or Services and physical access to secure areas. Without access control, information security is not possible.
Access (Physical)	The process of being able to enter designated secure areas.
Access Rights	The powers granted to users to create, change, delete or view information within a system according to a set of rules defined by the Information Owner, or the powers granted to user to physically access designated secure areas.
Accountability	The property that ensures that the actions of an individual or an institution may be traced uniquely to that individual or institution.
Audit	To conduct an independent review and examination of system records and activities in order to test the adequacy and effectiveness of controls and ensure compliance with established policies and operational procedures.
Auditability	Ensuring that protected and reliable records of system activity with security significance (e.g., logins, logouts, file accesses, security violations) are available.
Audit Logs	Computer files containing details of amendments to records that are necessary to track system activities.
Audit Trail	A chronological record of system activities to enable the reconstruction and examination of a sequence of events.
Authentication	Authentication provides the means of verifying the identity of an entity (user, process or resource).
Authorisation	Authorisation enables specification and subsequent management of allowed actions for a given system
Availability	Ensuring that Information Systems or Services are available when needed.
Backup	The process whereby copies of computer files are taken in order to allow recreation of the original in the event of a disaster.
Backup Power Generator	Diesel or petrol driven units, usually linked to an uninterruptible power supply, used to generate electricity in the event of a power failure.
Chain letter	A letter (or fax or email) directing recipients to send out multiple copies of it so its circulation increases exponentially. Such messages typically promise rewards for compliance, e.g.: blessings, good luck, money or merchandise. Some types of chain letters — specifically, those asking people to send money to other participants — are illegal.
Confidentiality	Confidentiality is the assurance that information is not disclosed to inappropriate entities (user, process or resource).

<i>Terms used</i>	<i>Definition</i>
Controls	Procedures or mechanisms that can reduce, or eliminate, the risk of a threat becoming an incident.
Denial of Service	A Denial of Service (DoS) is an attack (sometimes unintentional) whereby a client is denied the level of service expected. In a mild case, the impact can be unexpectedly poor performance, while in the worst case the system may become so overloaded as to cause a crash of the system. Typically associated with Internet and E-mail services but could also apply to other services.
Domain Name	The domain name identifies the location of an organisation or entity on the Internet.
Encryption	The process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality purposes.
Firewalls	Firewalls are security devices used to restrict access in communications networks. They prevent computer access between networks and only allow access to services which are expressly permitted.
Freeware	Software that is provided for free. Such software should be approached with caution as it could contain viruses or cause damage to company systems.
Forced Path	The principle of “Forced Path” in the networking environment is designed to allow network connections between two computers along a predetermined route only.
FTP	File Transfer Protocol. A common way of exchanging files, particularly in the UNIX environment but also over the Internet.
Hacker	An individual whose primary aim in life is to penetrate the security defences of large, sophisticated computer systems.
Identification	Identification is the process of distinguishing one entity (user, process or resource) from another
Impersonation	Pretending to be somebody else.
Information Integrity & Recoverability	Information Integrity & Recoverability ensures that information-processing resources behave in an appropriate or predefined manner in accordance with business purposes.
Information Systems or Services	The computer services and information sources used by our organisation to support its daily operations.
Integrity	Integrity refers to the correctness and appropriateness of the content and/or source of a piece of information
Internet Service Provider	A company that provides access to the Internet.
IP address	The IP address is the numeric address that guides all Internet traffic, such as e-mail and Web traffic, to its final destination.

<i>Terms used</i>	<i>Definition</i>
Logging	The process of recording events at the time that they occur.
Masquerading	Identifying yourself as somebody else.
Modem	Modulator, DEModulator. A piece of equipment that enables a computer to send transmissions through normal telephone lines.
News group	Discussion groups on the Internet where like-minded individuals can share information and ask questions on a particular topic.
Non-repudiation	The process that prevents any attempt by the sender to falsely deny sending the data, or subsequent attempts by the recipient to falsely deny receiving the data
Piggybacking	Gaining access to an Information System or Service or to a secure area via another user's legitimate access (e.g. using another user's UserID and password or using another user's access card)
PIN	Personal Identification Number. Code used by an individual so that he/she can access his/her device (like a telephone, fax, copier or ATM), but others can't.
PSTN	Public Switched Telephone Network. A voice and data communications service for the general public which uses switched lines e.g. the telephone network.
Risk analysis	A systematic method of identifying the value of an information system or service, the threats to that information system or service, and the vulnerability of the system or service to those threats.
Shareware	Software supplied on a "try before you buy" basis. Shareware has a reputation of causing conflicts with other software that may cause system problems.
Secure Areas	Areas within our organisation designated for the purpose of housing Information Systems or Services.
Secure Information Exchange	Secure Information Exchange protects transactions over internal or external communications channels.
Security Incident	A security incident is an alert to the possibility that a breach of security may be taking, or may have taken, place.
Spam	The electronic equivalent of Junk Mail.
Tail-gating	This occurs when one person enters through a controlled access point while another follows (or is let through) before the door closes or locks again.
Trap Door	A hidden software or hardware mechanism usually created for testing and troubleshooting that may be used to circumvent computer security.
Trojans	From Trojan Horse – a malicious, security breaking program that is disguised as something else such a screen saver, movie clip or game.

<i>Terms used</i>	<i>Definition</i>
Uninterruptible Power Supply	An Uninterruptible Power Supply (UPS) is a piece of hardware that contains its own batteries and can not only protect Information Systems or Services from sudden power surges but also continue its operation for up to 1 hour (or more) thus allowing an orderly system shutdown in the event of a prolonged power failure.
Virus	A form of malicious computer code that is potentially disruptive and may cause itself to transmit from computer to computer.
Visitor	Individual who has no regular access to our secure areas.
VPN	Virtual Private Network. A network that runs over a public network, but through the use of encryption maintains privacy.
Workstation	Computers issued to users.
Worms	A type of a virus that propagates itself over a network, reproducing itself as it goes.