Ecas AG's Information Security Policy

1. Introduction

Information Security is an essential part of our daily business. There is considerable risk to our business if Ecas AG does not:

- keep its information suitably confidential
- ensure it is available on a timely basis to those authorised to access it.

In addition it is the responsibility of everybody to ensure it is accurate, complete and can be relied on at all times, and cannot be refuted. This is a vital part of ensuring that we conduct our business lawfully (meeting regulatory, legal and contractual requirements), deliver a quality service and protect our client's reputation.

2. Scope

This Information Security Policy is mandatory across Ecas AG. All members of staff, contractors and agents who access Ecas AG information and systems are required to comply. Information may take the following forms, in particular: paper, pictures, video, sound, electronic data and spoken word.

3. Responsibilities

- Information Security cannot be delegated, everyone is responsible for appropriate information handling.
- Compliance with this Policy is the responsibility of everyone.
- We need to safeguard access to our systems and information, so that only authorized people can access or alter Information.

3.1 When Dealing with Confidential Information:

Information is a highly valuable asset and should only be used with due care.

- If you need to print confidential information, collect it from the printer immediately.
- Don't leave documents lying around if you are away from your desk.
- Don't give out information if you are not sure who you are communicating with, or whether that person should have access to the information.
- Do not leave confidential messages on answering machines or voicemail.
- Don't remove confidential information or equipment from the office without permission.
- Don't try to access systems, networks or information for which you have not been authorised.
- Dispose of information media securely using proper disposal facilities.
- Report the loss or theft of physical information or equipment.

3.2 When Working with Information Systems:

Get to know the applicable rules before accessing a specific information system.

- Protect confidential information appropriately for the medium involved (e.g. password protected transfer of reports via email).
- Never send confidential information across the Internet (or any third party network) without a security solution approved.
- Report actual or suspected breaches of Information.

We need to comply with relevant legislation and regulatory controls

- Banking secrecy, data protection and privacy laws must be complied with. Any unauthorised disclosure, alteration or deletion of personal data in breach of these laws may result in your prosecution. In Switzerland, the Banking Secrecy Law, the Data Protection Act, GDPR & the Post and Telecommunication Act covers all particularly confidential data (i.e., data relating to an identifiable individual) stored or processed by Ecas AG.

We need to ensure that security incidents are dealt with appropriately and that we can detect fraud, theft or criminal misuse of systems

- If you identify or suspect an Information Security weakness or incident, don't attempt to investigate it. Report it immediately to your Manager.