General Information Security Policy

Protect become.1 GmbH's informational and IT assets (including but not limited to all computers, mobile devices, networking equipment, software and sensitive data) against all internal, external, deliberate or accidental threats and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems;

Ensure information will be protected against any unauthorized access. Users shall only have access to resources that they have been specifically authorized to access. The allocation of privileges shall be strictly controlled and reviewed regularly.

Protect CONFIDENTIALITY of information. When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties;

Ensure INTEGRITY of information. Integrity of information refers to protecting information from being modified by unauthorized parties;

Maintain AVAILABILITY of information for business processes. Availability of information refers to ensuring that authorized parties can access the information when needed.

Comply with and, wherever possible, exceed, national legislative and regulatory requirements, standards and best practices;

Develop, **Maintain** and **Test** business continuity plans to ensure we stay on course despite all obstacles that we may come across. It is about "keeping calm and carrying on!";

Raise awareness of information security by making information security training available for all Employees. Security awareness and targeted training shall be conducted consistently, security responsibilities reflected in job descriptions, and compliance with security requirements shall be expected and accepted as a part of our culture;

Ensure that no action will be taken against any employee who discloses an information security concern through reporting or in direct contact with Information Security Management Leader, unless such disclosure indicates, beyond any reasonable doubt, an illegal act, gross negligence, or a repetitive deliberate or willful disregard for regulations or procedures;

Report all actual or suspected information security breaches to daniel.eberl@become1.de or by using the form linked in POL-17 Incident Management, Appendix B

1. Enforcement, Exceptions and Complaints

Non-conformance to policy and standard statements in this Policy could result in disciplinary action including, but not limited to, informal or formal warnings, up to termination of contract. Any exceptions to what is governed will require written authorization by email from Information Security Management Leader. Exceptions granted will be issued a policy waiver for a defined period of time. All target users of this Policy can submit complaints to its contents to Information Security Management Leader at any point. All complaints will be filed and processed accordingly where Information Security Management Leader will respond within 14 days of initial submission. Requests

for exceptions to this policy as well as complaint submissions will be addressed to Information Security Management Leader at daniel.eberl@become1.de.