



# Acceptable Information Technology Resource Use Policy

## Contents

1	Overview .....	1
2	Scope and application .....	1
3	General usage .....	2
4	Access, authentication and authorization .....	3
5	Electronic communications .....	3
7	Policy violations and consequences .....	4
8	Communication and training .....	5

## 1 Overview

This document outlines the Exponam policy for the acceptable use of Information Technology (IT) resources (which includes, but is not limited to software, hardware and networks) and infrastructure by any individuals working at Exponam.

## 2 Scope and application

This Policy applies to all individuals working at Exponam at all levels, including officers, managers, employees, consultants, contractors, trainees, or any other person associated with Exponam, regardless of their geographical location, jurisdiction of operation, job title or position (referred herein as users).

The Policy's clauses are applicable to all IT resources and all components of IT infrastructure, unless explicitly specified otherwise.



### 3 General usage

All Exponam IT resources and infrastructure are to be used:

- 3.1. In strict accordance with all the applicable laws and regulations of all levels.
- 3.2. Only in furtherance of Exponam business.
- 3.3. According to Exponam management guidance and authorization.

The following activities involving Exponam IT resources, infrastructure and Exponam owned storage devices are strictly prohibited:

- 3.4. Use of Exponam IT resources or infrastructure to offer products or services unless approved by Exponam.
- 3.5. Vandalism, disruption of services, attempting to circumvent security measures, spreading computer viruses/worms/malware, viewing/transmitting pornography, promoting hate sites/content.
- 3.6. Sending frivolous, obscene or harassing messages, as well as threatening, harassing, and intimidating others in any way.
- 3.7. Use of unauthorized wireless hotspots.
- 3.8. Use of unlicensed software, hardware or infrastructure components.
- 3.9. Unauthorized private, recreational (e.g., playing games), commercial, or political activities.
- 3.10. Unauthorized changes to the configuration and/or settings of any hardware, software or infrastructure components.
- 3.11. Storage and transmission of data on Exponam computers and networks, which is not owned legally by a user or distribution of this data to other users by copyright infringement is prohibited (for example movies, photos, music etc.).

Users of Exponam IT resources and infrastructure are hereby informed that:

- 3.12. Users are personally liable for any copyright violations or unauthorized charges incurred.
- 3.13. Users are responsible for any damage incurred by illegal or inappropriate uses of any Exponam IT resources and infrastructure.
- 3.14. Exponam reserves the right to monitor, track and log user activity and data on Exponam IT resources and infrastructure, as far as it is not in violation of any applicable law/regulation.
- 3.15. Exponam reserves the right to inspect and/or remove personal (that is, not relating to Exponam business) files or data stored on Exponam IT resources and infrastructure.
- 3.16. As stated in 3.14 and 3.15, users of Exponam IT resources and infrastructure should have no expectation of privacy for information sent or stored in it.



## 4 Access, authentication and authorization

Users of Exponam IT resources and infrastructure are obliged to adhere to the following rules of conduct in relation to access rights and permissions, authorization and authentication:

- 4.1. Access to all the Exponam IT resources and infrastructure remains at sole discretion of Exponam.
- 4.2. IT resource and infrastructure access is granted by Exponam based on the user's job function.
- 4.3. Attempting to access (log in) to another person's account, by using his/her username and password or other personal identification, is specifically prohibited.
- 4.4. Users are required to protect their username/password (as well as any other credentials and means for authorization and authentication) by not allowing others to access it and preventing it to be made publicly available.
- 4.5. Accessing another person's IT resources (e.g., to read someone else's e-mail) is prohibited unless it is explicitly authorized by Exponam management.
- 4.6. Unauthorized access, or unauthorized attempts to access IT resources may be illegal and result in criminal and civil liability for the violating user.
- 4.7. Sensitive or confidential data must not be placed in publicly accessible resources or otherwise made publicly available.

## 5 Electronic communications

Users of Exponam IT resources and infrastructure are obliged to adhere to the following rules of conduct in relation to electronic communications:

- 5.1. Users are not allowed to set up automatic forwarding of e-mails and other channels of communications from Exponam to personal addresses/accounts unless explicitly approved by the Exponam management.
- 5.2. Exponam IT resources and infrastructure may not be used to send chain letters, solicitations/advertisements, etc.
- 5.3. Mass e-mail, instant message or voice mail from any user to any party must first be approved by Exponam management. All non-business related mass communications except for Exponam sanctioned events are not permitted regardless of the electronic communications channel chosen
- 5.4. Exponam IT resources and infrastructure are prohibited to be used for illegal or inappropriate electronic communications, regardless of tools, applications, platforms or protocols involved. Examples of prohibited communications include (but are not limited to):
  - Obscene, profane, lewd, vulgar, disrespectful, threatening or defamatory



- language.
  - Knowingly introducing computer viruses, Trojan horses, worms, or similar mechanisms.
  - Copyright infringement or plagiarism.
- 5.5. Users are not allowed to interfere with or deny electronic communications system services to any user.
- 5.6. Users are not allowed to export software, technical information, or technology in violation of International or regional export control laws.
- 6** Users are not allowed to effect security breaches or disruptions of any electronic communications system. This includes, but is not limited to tampering with the security of company owned computers, network equipment, services or files. Hardware, software and network
- Users of Exponam IT resources and infrastructure are obliged to adhere to the following rules of conduct in relation to their use of software, hardware and networks:
- 6.1. Activities unrelated to approved business needs that result in excessive use of network bandwidth, server storage, or system time are forbidden (this specifically includes downloading and storing of video/audio files).
  - 6.2. Software may be used only in accordance with license agreements.
  - 6.3. Unauthorized use of personal laptops, tablets and any other personal devices on the internal wired network is strictly prohibited.
  - 6.4. Unauthorized modification of operating systems, application software, or network software on any component of the Exponam infrastructure is strictly forbidden.
  - 6.5. Tampering (altering from intended purpose) with terminals, computers, printers or any other associated peripherals that are owned or leased by Exponam is strictly forbidden.
  - 6.6. Unauthorized removal of computers, disks, peripherals and data from a Exponam facility is strictly forbidden except for those devices which are issued explicitly for the purpose of mobility (e.g., laptops, mobile phones).

## 7 Policy violations and consequences

- 7.1. Violation of this Policy could result in the imposition of disciplinary action up to and including termination.
- 7.2. Exponam reserves the right to close or suspend a user's access to IT resources and infrastructure at any time.
- 7.3. Disciplinary action taken by Exponam does not preclude prosecution in cases of criminal misconduct under applicable laws and regulations.



## 8 Communication and training

Training on this policy is included in the on-boarding process for all new employees. All existing employees will receive regular, relevant training on how to implement and adhere to this policy. Exponam management at all levels is responsible for ensuring those reporting to them is made aware of and understand this policy.