#09

Policy 政策
Information security
信息安全

Corporate social responsibility

This leaflet is devoted to warnings about the various cyber-attacks and the best practices to put in place.

1. WHAT IS INFORMATION SYSTEMS SECURITY?

This means ensuring the security of all our assets (site, people, hardware, network, software and organisation).

2. THE DIFFERENT TYPES OF ATTACK

There are 4 main types of attacks that we experience at Altyor:

- **Ransomware:** data encryption
- **Phishing:** sending counterfeit emails
- **Spear phishing:** phishing based on the personal / professional network
- **President's Attack:** convincing a company's employee to make a transfer to a third party

3. THE ESSENTIAL RULES

- ☑ **Choose your passwords carefully**
- ☑ **Choose Altyor Wi-Fi access**
- ☑ **Be as careful with your smartphone or tablet as with your computer**
- ☑ **Protect your data when you travel (password)**
- ☑ **Be careful when using email**
- ☑ **Download programs from official publisher websites (always ask the IS for validation)**
- ☑ **Be careful when making payments on the Internet**
- ☑ **Separate personal and professional uses**
- ☑ **In case of doubt, always report the information to IS**

4. OUR COMMITMENTS

Altyor undertakes to:

- Responsible, fair and transparent collection, use and disclosure of personal data (any information relating to an individual who can be directly or indirectly identified) of employees, in accordance with applicable laws, standards and norms.
- Process data for the legitimate purposes explicitly specified to the data subject when the Group collected it.
- Collect and process only as much data as necessary for the specified purposes. Personal data is mainly used for human resources, IT, occupational health and safety, labor relations, infrastructure management and audits.
- Use reasonable organizational, technical and administrative measures to protect the personal data under its control.

5. HOW TO REPORT BACK?

Your alert will be processed as soon as possible via your manager, the IT department, the HR department or anonymously via:

https://altyor.com/csr-commitments/

Sanction: it is important to report information about attacks, otherwise it can be considered as professional misconduct

6. REPORTING

Altyor is committed to monitoring its cybersecurity performance and, to this end, tracks the following indicators

- Number of confirmed IT security incidents
- Number of incidents reported through the alert procedure

7. PERIMETER

This policy applies to all Altyor Group entities and all external stakeholders of the Group.

8. RESPONSIBILITY

The CSR committee is responsible for defining the cybersecurity policy. The IT department is responsible for ensuring that it is properly implemented.

9. COMMUNICATION

This policy is communicated annually to all employees through the usual company channels, including internal company rules and the company intranet, and is presented to all new staff members on induction. This policy is also distributed to external stakeholders and is available on the Altyor website.

10. CONTACT

For more information, please contact Alexis Lutun alutun@altyor.com or send an email to contact@altyor.com.

11. REVIEW HISTORY TABLE

This Policy is reviewed annually or in the event of a change in related government policy or significant changes in the company's operations.

This Policy was last approved on 22nd of December 2023 by Yanis Cottard, President of the Altyor Group.

Policy version	Description of change	Date of change
A	N/A	January 2023
B	Adding KPIs to the policy	July 2023
C	Renamed of the policy “Information security" and adding commitments to employees data	December 2023

这部分主要是对各种网络攻击的警告，以及应采取的最佳做法的政策。

1. 什么是信息系统安全？

这意味着要确保我们所有资产（场地、人员、硬件、网络、软件和组织）的安全。

2. 不同类型的攻击

我们在 ALTYOR 经历的攻击主要有 4 种类型。

- 勒索软件：数据加密
- 网络钓鱼：发送伪造的电子邮件
- 鱼叉式网络钓鱼：基于个人/职业网络的网络钓鱼
- 总统攻击：说服公司的员工向第三方转账

3. 基本规则

- ☑ 谨慎选择你的密码
- ☑ 选择 **Altyor Wi-Fi 接入**
- ☑ 使用智能手机或平板电脑要像使用电脑一样谨慎
- ☑ 旅行时保护您的数据（密码）
- ☑ 使用电子邮件时要小心
- ☑ 从官方出版商的网站上下载程序（一定要询问 IS 的验证）。
- ☑ 在互联网上进行支付时要小心
- ☑ 将个人使用和专业使用分开
- ☑ 如有疑问，一定要向 IS 报告信息。

4. 我们的承诺

阿尔蒂尔承诺

- 根据适用的法律、标准和规范，负责任、公正且透明地收集、使用和披露员工的个人数据（任何与可直接或间接识别的个人相关的信息）。
- 按照集团收集数据时向数据当事人明确说明的合法目的处理数据。
- 只收集和处理指定用途所需的数据。个人数据主要用于人力资源、IT、职业健康与安全、劳动关系、基础设施管理和审计。
- 采取合理的组织、技术和行政措施，保护其控制下的个人数据。

5. 如何报告？

你的警报将通过你的经理、IT 部门、人力资源部门或通过匿名方式尽快处理。

https://altyor.com/csr-commitments/

制裁：报告有关攻击的信息是很重要的，否则会被认为是职业不当行为。

6. 报告

阿尔泰尔致力于监测其网络安全性能，并为此跟踪以下指标

- 经确认的信息技术安全事件的数量
- 通过警报程序报告的事件数量

7. 周期

本政策适用于阿尔泰尔集团的所有实体和集团的所有外部利益相关者。

8. 责任

企业社会责任委员会负责确定网络安全政策。IT 部门负责确保该政策的正确实施。

9. 沟通

本政策每年通过公司的常规渠道，包括公司的内部规定和公司的内部网，向所有员工传达，并在所有新员工入职时介绍。本政策也会分发给外部利益相关者，并在 Altyor 网站上公布。

10. 联系方式

欲了解更多信息，请联系 Alexis Lutun alutun@altyor.com 或发送电子邮件至 contact@altyor.com。

11. 审查历史表

本政策每年或在相关政府政策发生变化或公司业务发生重大变化时进行审查。

本政策最后由阿尔泰尔集团总裁 Yanis Cottard 于 2023 年 12 月 22 日。

政策版本	变更说明	修改日期
A	N/A	2023 年 1 月
B	在政策中添加关键绩效指标	2023 年 7 月
C	将政策更名为 "信息安全"，并增加对员工数据的承诺	2023 年 12 月