INFORMATION SECURITY GUIDE

for External Partners, Suppliers, and Contractors

INTRODUCTION

This guide defines the basic information security requirements for external partners, suppliers, and contractors who have a contractual relationship with the Alpiq Hungary Group, have access to its administrative or operational IT systems, or contribute to the operation of the IT/OT environment. The purpose of this document is to ensure the protection of Alpiq's data assets, business processes, and IT and cyber-physical systems during collaborative work.

The Alpiq Group is committed to maintaining a high standard of information security commensurate with relevant risks. It complies with NIS2 regulations and expects all its external partners to consistently adhere to the requirements applicable to supply chain participants. Compliance with the rules set forth in this guide is mandatory for all persons and organizations – as detailed above – who perform activities on behalf of or in the interest of Alpiq.

1. GENERAL SECURITY REQUIREMENTS

1.1 Confidentiality Obligation

All external partners must sign a confidentiality agreement prior to entering into a contract. This obligation applies to all information encountered during cooperation with Alpiq. The confidentiality obligation remains in effect for the period specified by law even after the contract has ended.

Confidential information includes, in particular:

- Business plans, strategies, and financial data;
- Technical documentation and technological solutions, configuration parameters;
- Customer and partner data;
- Internal organizational information;
- IT system architecture and security measures.

1.2 Personnel Security

External partners must ensure that the employees they delegate have undergone appropriate background checks, security awareness training, and professional training. All affected employees must accept the declaration at regarding compliance with the provisions of Alpiq's Information Security Guidelines.

External partners are required to immediately notify Alpiq's designated contact person if an employee's employment is terminated or their access rights change.

2. DATA PROTECTION REQUIREMENTS

2.1 Processing of Personal Data

The personal data of Alpiq's customers and employees may only be used for the purposes and to the extent specified in the contract. All data processing activities must be conducted in accordance with the provisions of the GDPR.

Mandatory measures:

- Personal data may only be stored and transmitted in encrypted form;
- Access to the data must be restricted to the minimum necessary group of individuals;
- All data processing operations must be documented;
- In the event of a data breach, Alpiq's local data protection officer must be notified within 24 hours.

2.2 Protection of Business Data

Alpiq's business data must be treated as strictly confidential. This information may not be shared with third parties without prior written authorization and may only be used to perform the tasks specified in the contract.

Prohibited activities:

- Making copies of business data for personal use;
- Sharing information with competitors;
- Using data to gain a competitive advantage;
- Processing data in a public place without adequate protection.

3. IT SECURITY REQUIREMENTS

3.1 Access Management

Access to Alpiq's IT systems is only possible via pre-approved user accounts, for which each user must have a unique ID and a strong password.

Password requirements:

- Minimum length of 12 characters;
- Use of uppercase letters, lowercase letters, numbers, and special characters;
- Mandatory password change every 90 days;
- Reuse of previous passwords is not permitted.

User accounts must not be shared with other individuals. Alpiq logs all access events and conducts regular, targeted audits.

3.2 Device Security Requirements

Devices connected to Alpiq's IT or OT network must comply with the security requirements set by the operator:

Mandatory security software:

- Installation and operation of up-to-date antivirus protection;
- Regular installation of operating system security updates;
- Activation and proper configuration of a personal firewall;
- Use of data encryption for sensitive information.

Prohibited activities:

- Installing software from unknown or illegal sources;
- Unauthorized connection and use of devices containing data storage media (e.g., USB drives, mobile phones);
- Connecting to unauthorized networks.

3.3 Remote Access Security

Remote access to Alpiq's IT or OT systems is permitted only via a secure VPN or other encrypted connection approved by the client that enables remote work. When working remotely, special attention must be paid to environmental security.

Rules for remote work in brief:

- Connections may only be initiated and work performed in a closed (bridge mode excluded), controlled, and up-to-date environment;
- The screen must be protected from unauthorized viewing;
- The use of public Wi-Fi networks is not permitted.

4. PHYSICAL SECURITY MEASURES

4.1 Site Access

Access to Alpiq premises is permitted only to persons who have been registered and approved in advance. All visitors must be accompanied and must wear a visitor badge.

Entry rules:

- Advance registration is mandatory;
- Identification must be verified before an access pass is issued;
- An escort must be provided by the host;
- Access to security or operational areas requires special authorization and protective equipment.

4.2 Document Management

Paper-based documents must be handled and stored in accordance with the fundamental rules of confidentiality, integrity, and availability. Confidential documents and data storage media must not be left unattended.

Document management rules:

- Confidential documents must be stored out of reach of unauthorized persons;
- Making physical or electronic copies requires the data owner's permission;
- Disposal must be carried out using a document shredder that ensures irrecoverability;
- Documents containing confidential information may be transported in sealed envelopes or document carriers.

5. COMMUNICATION SECURITY REQUIREMENTS

5.1 Email Security

When communicating via email, special attention must be paid to the protection of business information. Confidential information may only be sent via encrypted email.

Email security rules:

- Do not open attachments that appear suspicious;
- Encryption of confidential information (e.g., using PGP encryption or a password-protected ZIP file) is mandatory;
- The use of personal email addresses for business purposes is not supported.

5.2 Use of Social Media

Sharing business or internal information related to Alpiq on social media is strictly prohibited. This applies to project details, employees, and business processes alike.

6. INCIDENT MANAGEMENT OBLIGATIONS

6.1 Reporting Security Incidents

All security incidents or suspicious activities must be reported immediately to Alpiq's Information Security Officer at ibf.hun@alpiq.com.

Incidents to be reported:

- Data loss or data leakage affecting the client's data assets;
- Attempts to gain unauthorized access to the client's or contractor's data assets;
- Detection of a virus infection or malicious software in a work environment that may come into direct or indirect contact with Alpiq's IT or OT infrastructure;
- Physical security incidents (e.g., unauthorized entry, natural disasters);
- Loss or theft of devices.

6.2 Obligation to Cooperate

In the event of a security incident, external partners must fully cooperate with Alpiq's investigation. This includes providing the necessary information and supporting recovery efforts.

7. COMPLIANCE AND AUDITING

7.1 Audit Rights

Alpiq reserves the right to verify the information security compliance of external partners. This includes on-site audits with pre-agreed scope and the review of documentation submitted as evidence.

7.2 Consequences of Breach of Contract

A proven violation of information security requirements constitutes a material breach of contract, which may result in immediate termination of the contract and a claim for damages.

8. TRAINING AND AWARENESS REQUIREMENTS

8.1 Mandatory training

All employees of external partners must complete Alpiq's basic information security (e-learning) training before commencing work. This training, which includes mastering the content of this document and successfully answering a set of review questions, must be repeated annually.

9. TECHNOLOGICAL REQUIREMENTS

9.1 Software Use

Only legally licensed and security-checked software may be used on Alpiq projects. Security updates for the software must be installed regularly.

9.2 Data Backup and Recovery

Regular backups must be made of critical data. Backup procedures must be tested, and recovery plans must be kept up to date to minimize the risk of data loss.

10. TERMINATION OF THE AGREEMENT

10.1 Return of Data

Upon termination of the contract, all data, information, and documents owned by Alpiq must be returned to the client or, by mutual agreement with the client, irretrievably destroyed.

10.2 Termination of Access

All IT access must be terminated immediately upon the expiration or termination of the contract.

This guideline is an excerpt from the Alpiq Hungary Group's Information Security Policy. Compliance with the requirements contained herein is mandatory for all external partners. If you have any questions, please contact Alpiq's Information Security Officer at ibf.hun@alpiq.com.

Effective Date: the date of signing the contract.

Review: annually or in the event of significant changes.