SUPPLIER RELATIONSHIP POLICY

Policy

It is the policy of AzteQ Group Ltd to demonstrate to our stakeholders that the choices we make regarding suppliers are done with due diligence and that the ongoing monitoring and review of the service supplied are performed in an effective way.

The purpose of this document is to set out the Organisation's information security policy in the area of supplier relationships.

Introduction

AzteQ Group Ltd and its core business exist in a wider economic environment in which effective relationships with suppliers are critical to its continued success. However, recent information security breaches have shown that sometimes a third-party supplier can represent a significant weakness in the defences of our information assets.

It is very important therefore that our relationships with suppliers are based on a clear understanding of our expectations and requirements in the area of information security. These requirements must be documented and agreed in a way that leaves no doubt about the importance we place on the maintenance of effective controls to reduce risk.

Responsibilities

1. Every member of staff is responsible for ensuring that this Policy is complied with. Particular responsibility lies with those with direct responsibility for supplier relationships and supplier operations.
2. All of the Organisation's employees are responsible for using the Organisation's facilities in a responsible manner in accordance with this Policy.

General Provisions

In general, information security requirements will vary according to the type of contractual relationship that exists with each supplier and the goods or services delivered.

However, the following will generally apply:

1. The information security requirements and controls must be formally documented in a contractual agreement which may be part of, or an addendum to, the main commercial contract
2. Separate Non-Disclosure Agreements must be used where a more specific level of control over confidentiality is required
3. Appropriate due diligence must be exercised in the selection and approval of new suppliers before contracts are agreed
4. The information security provisions in place at existing suppliers (where due diligence was not undertaken as part of initial selection) must be clearly understood and improved where necessary
5. Remote access by suppliers must be via approved methods that comply with our information security policies

6. Access to AzteQ Group Ltd information must be limited where possible according to clear business need
7. Basic information security principles such as least privilege, separation of duties and defence in depth must be applied
8. The supplier will be expected to exercise adequate control over the information security policies and procedures used within sub-contractors who play a part in the supply chain of delivery of goods or services to AzteQ Group Ltd
9. AzteQ Group Ltd will have the right to audit the information security practices of the supplier and, where appropriate, sub-contractors
10. Incident management and contingency arrangements must be put in place based on the results of a risk assessment
11. Awareness training will be carried out by both parties to the agreement, based on the defined processes and procedures.

The selection of required controls must be based upon a comprehensive risk assessment taking into account information security requirements, the product or service to be supplied, its criticality to the Organisation and the capabilities of the supplier.

Cloud Services

Cloud service providers (CSPs) must be clearly recognised as such so that the risks associated with the CSP's access to and management of AzteQ Group Ltd cloud data may be managed appropriately.

Due Diligence

Before contracting with a supplier, it is incumbent upon AzteQ Group Ltd to exercise care in reaching as full an understanding as possible of the information security approach and controls the company has in place. It is important that the all reasonable and appropriate checks are made so that all of the required information is collected, and an informed assessment can be made.

This is particularly important where cloud computing services are involved, as legal considerations regarding the location and storage of personal data must be considered.

Addressing Security Within Supplier Agreements

Once a potential supplier has been positively assessed the information security requirements of AzteQ Group Ltd must be reflected within the written contractual agreement entered into. This agreement must take into account the classification of any information that is to be processed by the supplier (including any required mapping between AzteQ Group Ltd information classifications and those in use within the supplier), legal and regulatory requirements and any additional information security controls that are required.

For cloud service contracts, information security roles and responsibilities must be clearly defined in areas such as backups, incident management, vulnerability assessment and cryptographic controls.

Appropriate legal advice must be obtained to ensure that contractual documentation is valid within the country or countries in which it is to be applied.

Evaluation of Existing Suppliers

For those suppliers that were not subject to an information security due diligence assessment prior to an agreement being made, an evaluation process must be undertaken in order to identify any required improvements.

Monitoring and Review of Supplier Services

In order to focus resources on the areas of greatest need, suppliers are categorised based on an assessment of their value to the Organisation.

Each supplier will be placed into one of the following four categories:

- Commodity
- Operational
- Tactical
- Strategic

The recommended frequency of supplier review meetings between AzteQ Group Ltd and each supplier will be determined by the supplier's category according to the following table:

Supplier Category	Recommended Meeting Frequency
Commodity	None
Operational	On contract renewal
Tactical	Annually
Strategic	Monthly/Quarterly

Each supplier has a designated contract manager within AzteQ Group Ltd who is responsible for arranging, chairing and documenting the meetings.

The performance of strategic suppliers will be monitored on a regular basis in line with the recommended meeting frequency. This will take the form of a combination of supplier-provided reports against the contract and internally produced reports.

Where possible, a frequent cross-check will be made between the supplier reports and those created internally in order to make sure the two present a consistent picture of supplier performance. Both sets of reports are reviewed at supplier meetings and any required actions agreed.

Changes Within Contracts

Changes to services provided by suppliers will be subject to the AzteQ Group Ltd change management process. This process includes the requirement to assess any information security implications of changes so that the effectiveness of controls is maintained.

Contractual Disputes

In the event of a contractual dispute, the following initial guidelines must be followed:

- The Head of Finance and/or CEO must be informed that a dispute exists
- The Head of Finance and/or CEO will then decide on next steps, based on an assessment of the dispute
- Where applicable, legal advice should be obtained via the Head of Finance and/or CEO
- All correspondence with the supplier in dispute must be in writing and with the approval of the Head of Finance and/or CEO

- An assessment of the risk to the Organisation should be carried out prior to escalating any dispute, and contingency plans put in place.

At all times the degree of risk to the business must be managed and if possible minimised.

End of Contracts

The following process will be followed for scheduled end-of-contract, early end of contract or transfer of contract to another party:

- The end of contract will be requested in writing within the agreed terms
- Transfer to another party shall be planned as a project and appropriate change control procedures followed
- An assessment of the risk to the Organisation should be carried out prior to ending or transferring the contract, and contingency plans put in place
- Any budgetary implications shall be incorporated into the financial model.

The various aspects of ending a contract must be carefully considered at initial contract negotiation time.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updated dates