**ISMS Supplier Relationships**

**Doc A15**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 ISMS Supplier Relationships 3

1.1 Scope 3

1.2 Responsibilities 3

2 Policy statement 3

3 Procedures 3

3.1 Addressing security within supplier agreements 3

3.2 Information and communication technology supply chain 4

3.3 Monitoring and review of supplier services 6

3.4 Managing changes to supplier services 6

4 Document Control and Approval 8

4.1 Distribution 8

4.2 Version Information 8

# ISMS Supplier Relationships

## Scope

This procedure ensures the protection of the organization’s assets that are accessible by suppliers.

## Responsibilities

The Chief Financial Officer (CFO) is responsible for this procedure.

Executives, Directors and Managers are responsible for ensuring this procedure is understood and complied with within the organization.

Supplier owners are responsible for following the requirements of this procedure.

## 

# Policy statement

All suppliers that may access, share, process or store Wacky Widget’s information or Wacky Widget’s premises and where such information is held or processed will be subject to a documented agreement.

Each supplier will have a nominated relationship owner who is responsible for:

* Ensures that such an agreement is in place
* Includes controls as required to ensure the security of information including
  + storage locations
  + sub-processors

Prior to entering into any agreement Suppliers and clients must sign a confidentiality agreement as identified in an NDA (Non-disclosure agreement).

A risk assessment is conducted by the supplier owner, in conjunction with the Risk and Compliance Team, to identify the appropriate controls.

Suppliers are monitored for performance against the agreement by the relationship owner at least annually. Any deficiencies are brought to the attention of the supplier and an agreed action plan may be implemented to eliminate these shortfalls, or terminate the contract.

# Procedures

## Addressing security within supplier agreements

When drawing up a documented agreement with a supplier, for either a new or revised contract, the following is considered and included in the agreement as appropriate based upon the risk assessment:

1. **Description of Service or Information Shared:** 
   * Document the information or service to be provided or accessed.
   * Methods of providing or accessing the service or the information.
2. **Data Classification:** 
   * Classification of information according to the organization’s classification scheme.
   * (If necessary) mapping between the organization’s own classification scheme and the classification scheme of the supplier.
3. **Legal and Regulatory Requirements**:
   * Where required, GDPR requirements are met
   * Data protection
   * Intellectual property rights and copyright
   * A description of how it will be ensured that they are met.
4. **Obligations:**
   * Supplier’s obligations to comply with Wacky Widget’s security requirements.
   * Agreement on each contractual party responsibility to implement a set of controls including access control, performance review, monitoring, reporting and auditing.
5. **Rules of Acceptable Use** **of Information**
   * Including unacceptable use if necessary;
6. **Authorized Personnel**
   * Explicit list of supplier personnel authorized to access
   * Personnel authorized to receive the organization’s information
     1. procedures or conditions for
        1. authorization
        2. removal of the authorization
        3. access to or receipt of the Wacky Widget’s information
7. **Information security policies**
   * Policies relevant to the specific contract
8. **Incident Response**
   * Incident management requirements and procedures

\* especially notification and collaboration during incident remediation

1. **Sub-Contracting**
   * Relevant regulations for sub-contracting
   * Controls that need to be implemented;
2. **Point of Contact**
   * Relevant agreement partners
   * Contact person for information security issues
3. **Audit**
   * Supplier’s obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
4. **Business Continuity**
   * Provisions in respect of continuity of service should a significant incident occur which adversely affects the suppliers ability to comply with the contractual agreement

The documented agreement must be approved by both parties (or their authorized representative(s)). A copy of the agreed agreement is retained by Wacky Widget’s Procurement Manager in a secure location to which access is restricted.

## Information and communication technology supply chain

Where a supplier is likely to further subcontract some or all of the service provided to Wacky Widget then the following additional provisions are in place,

1. Requirement to report to Wacky Widget any new sub-contractors or change in current sub-contractors, prior to them working with Wacky Widget data.
2. Requirements that the supplier propagates Wacky Widget security requirements throughout the supply chain involved in the supply of the service including adoption of appropriate security practices.
3. Defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

These additional requirements are included in the agreement as appropriate

## 

## Monitoring and review of supplier services

The relationship owner reviews the performance of the supplier against the documented agreement. This review should occur at least once per year.

The relationship owner maintains a record of the review.

It should be noted that some suppliers of essential services may be reviewed at more frequent intervals. The record of review may be in the form of meeting minutes.

The review should include as appropriate the following:

1. Service performance levels to verify adherence to the agreements;
2. Review service reports produced by the supplier
3. Review any information security incidents and the supplier’s response to such incidents
4. Review of suppliers operational failures, tracing of faults and disruptions related to the service delivered;
5. Review of supplier’s response to any identified problems;
6. Review information security aspects of the supplier’s relationships with its own suppliers;
7. Ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster

## Managing changes to supplier services

Where either party (Wacky Widget or the supplier) wish to make a change to an existing agreement then the process is:

The relationship owner reviews the proposed change in consultation with the supplier and appropriate Wacky Widget personnel, including the procurement manager and a legal representative.

The risk of the change is reviewed by the relationship owner in consultation with the Risk and Compliance Team if appropriate.

The change is assessed for technical implications to ensure that the change will not adversely impact Wacky Widget.

# Document Control and Approval

The Risk and Compliance Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

This document was approved by Chief Technology Officer and is issued on a version controlled basis.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |