Supply Chain Security Principles

Implementing an effective control and oversight of the University supply chain.

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Mick Jenkins
Chief Information Security Officer

Pekka Kahkipuro
Chief Information Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	02/09/2019

Document Approval

The contents of this document are Protect to Brunel University London (BUL). Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

A Clarke	
Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Section 1- Purpose of this document

1.1 Overview

The 12 Supply chain security principles will provide the University with an improved awareness of supply chain security, as well as helping to raise the baseline level of competence in this regard, through the continued adoption of good practice.

The University relies upon suppliers to deliver products, systems, and services, however, the University supply chains can be large and complex, involving many suppliers doing many different things.

Effectively securing the supply chain can be hard because vulnerabilities can be inherent, or introduced and exploited at any point in the supply chain. A vulnerable supply chain can cause damage and disruption.

12 Principles
These principles have been designed to help gain and maintain the necessary level of control over the University supply chains.

1.2 Scope

This document addresses the requirements for Supply chain security Principles of the Brunel University London Security position.

Section 2 – Supply Chain considerations

2.1 What information is to be stored

It is important to consider what information / data the Supply chain is party to. BUL classifies information according to the classifications standard listed below:

- **UNCLASSIFIED**
- **PROTECT**
- **UNIVERSITY CONFIDENTIAL**

Note: For more information please see BUL-PROC-08-02 Information Classification and BUL-POL-08-02 Information Classification

Section 3 – 12 Supply chain security Principles

3.0 The principles of supply chain security

This guidance proposes a series of 12 principles, designed to help establish effective control and oversight of the University supply chain.

The principles have been divided into four separate stages:

1. Understand the risks
   The first three principles deal with the information gathering stage.
2. Establish control
   This section's principles will help gain and maintain control of the supply chain.
3. Check arrangements
   The University will need to gain confidence in the approach to establishing control over the supply chain.
4. Continuous improvement
   As the University supply chain evolves, it will be necessary to continue improving and maintaining security

Understand the Risk

The first three principles deal with the information gathering stage.
It is essential that until the University has a clear picture of the full supply chain, it will be very hard to establish any meaningful control over it. It is necessary to invest an appropriate amount of effort and resource to achieve this.

3.1 Principle 1 - Understand what needs to be protected and why

You [Supply Chain Owner / Procurement] should know:

- *The sensitivity of the contracts you let or will be letting.*
- *The value of your information or assets which suppliers hold*, will hold, have access to, or handle, as part of the contract.
- Think about the level of protection you need suppliers to give to your assets and information, as well as the products or services they will deliver to you as part of the contract.

3.2. Principle 2 - Know who your suppliers are and build an understanding of what their security looks like

You [Supply Chain Owner / Procurement] should know:

- *Who your suppliers are*. You will need to think about how far down your supply chain you need to go to gain understanding and confidence in your suppliers.
  You may have to rely on your immediate suppliers to provide information about sub-contractors, and it may take some time to ascertain the full extent of your supply chain.
- *The maturity and effectiveness of your suppliers' current security arrangements*
- *What security protections you have asked your immediate suppliers to provide, and what they, in turn, have asked any sub-contractors to do*:
  - Determine whether or not your suppliers and their sub-contractors have provided the security requirements asked of them.
  - Understand what access (physical and logical) your suppliers have to your systems, premises and information and how you will control it.
  - Understand how your immediate suppliers, control access to, and use of, your information and/or assets - including systems and premises, by any sub-contractors they employ.

  You should focus your efforts in this area on those parts of your suppliers' business or systems that are used to handle your contract information, or to deliver the contracted product or service.

3.3. Principle 3 - Understand the security risk posed by your supply chain

Assess the risks these arrangements pose to your information or assets, to the products or services to be delivered, and to the wider supply chain.

Sources of risk

Risks to and from the supply chain can take many forms. For example, a supplier may fail to adequately secure their systems, may have a malicious insider, or a supplier's members of staff may fail to properly handle or manage your information.

It could be that you have poorly communicated your security needs so the supplier does the wrong things, or the supplier may deliberately seek to undermine your systems through malicious action (this may be under state influence for national security applications).

Use the best information you can to understand these security risks. For example:

- Common cyber attacks - reducing the impact
- Insider data collection report
- Insider risk assessment

Getting mitigation right

Understanding the risk associated with the supply chain is key to ensuring security measures and mitigations are proportionate, effective and responsive.

Use this understanding to decide the appropriate levels of protection you will expect suppliers across your supply chain to provide for any contract information, and contracted products or services.

Plan of action

It may be useful to group different lines of work, contracts or suppliers into different risk profiles, based on considerations such as: the impact on your operations of any loss, damage or disruption, the capability of likely threats, the nature of the service they are providing, the type and sensitivity of information they are processing etc. Each profile will require slightly different treatment and handling to reflect your view of the associated risks. This may make things easier to manage and control.

You [Supply Chain Owner / Procurement] should document these decisions and share them with suppliers. For example, you may decide that contracts which provide basic commodities such as stationery, or cleaning services require very different approaches to management to those that provide critical services or products.

Establish control

This section's principles will help you gain and maintain control of your supply chain.

Once you gain better control of your supply chain you will be able to analyse strategic risks to it. For example to:

- Identify any suppliers who continually fail to meet your security and performance expectations.
- Identify critical assets and any over-reliance on single suppliers. This will help you to build further diversity and redundancy into your planning.

3.4. Principle 4 - Communicate your view of security needs to your suppliers

Ensure that suppliers understand their responsibility to provide appropriate protection for your contract information and contracted products and services and the implications of failing to do so.

Ensure suppliers adhere to their security responsibilities and include any associated security requirements in any sub contracts they let.

You [Supply Chain Owner / Procurement] should decide whether you are willing to permit your suppliers to sub-contract and delegate authority to do so appropriately.

Give suppliers clear guidance on the criteria to use for such decisions (e.g. the types of contract that they can let with little/no recourse to you, and those where your prior approval and sign-off must always be sought).

3.5. Principle 5 - Set and communicate minimum security requirements for your suppliers

You [Supply Chain Owner / Procurement] should set minimum security requirements for suppliers which are justified, proportionate and achievable.

Ensure these requirements reflect your assessment of security risks, but also take account of the maturity of your suppliers' security arrangements and their ability to deliver the requirements you intend to set.

It may also be sensible to identify circumstances where it would be disproportionate to expect suppliers to meet the minimum security requirements. For example, this may only be relevant for those suppliers who only need ad hoc, or occasional access to limited and specific data, and/or access to your premises.

You [Supply Chain Owner / Procurement] should document these considerations and provide guidance on the steps you intend to take to manage these engagements. This approach could help reduce your workload and avoid creating additional, unnecessary work for these parties.

Case by case

Consider setting different protection requirements for different types of contracts, based on the risk associated with them - avoid situations where you force all your suppliers to deliver the same set of security requirements when it may not be proportionate or justified to do so.

Explain the rationale for these requirements to your suppliers, so they understand what is required from them.

Include the minimum security requirements in the contracts you have with suppliers and in addition, require that your suppliers pass these down to any sub-contractors they might have.

3.6. Principle 6 - Build security considerations into your contracting processes and require that your suppliers do the same

Build security considerations into the normal contracting processes. This will help you [Supply Chain Owner / Procurement] to manage security throughout the contract, including termination and the transfer of services to another supplier.

Evidence

Require prospective suppliers to provide evidence of their approach to security and their ability to meet the minimum security requirements you have set at different stages of the contract competition.

Providing support

Develop appropriate supporting guidance, tools and processes to enable the effective management of the supply chain by you and your suppliers, at all levels.

You [Supply Chain Owner / Procurement] should:

- Ensure the security considerations built into the contracts are proportionate and align with the various stages of the contracting process.
- Require their adoption in contracts and train all parties on their use.
- Check that supporting guidance, tools and processes are being used throughout the whole of your supply chain.
- Require contracts to be renewed at appropriate intervals, and require reassessment of associated risks at the same time.
- Seek assurance that your suppliers understand and support your approach to security and only ask them to take action or provide information where it is necessary to support the management of supply chain security risks.
- Ensure that contracts clearly set out specific requirements for the return and deletion of your information and assets by a supplier on termination or transfer of that contract.

3.7. Principle 7 - Meet your own security responsibilities as a supplier and consumer

Ensure that You [Supply Chain Owner / Procurement] enforce and meet any requirements on you as a supplier.

Provide upward reporting and pass security requirements down to sub-contractors.

Welcome any audit interventions the customer might make, tell them about any issues you are encountering and work proactively with them to make improvements.

Challenge your customers if guidance covering their security needs is not forthcoming, and seek assurance that they are they happy with the measures you are taking.

3.8. Principle 8 - Raise awareness of security within your supply chain

Explain security risks to suppliers using language they can understand. Encourage them to ensure that key staff (e.g. procurement, security, marketing) are trained on, and understand these risks, as well as their responsibilities to help manage them.

Set goals
Establish supply chain security awareness and education for appropriate staff.

Information sharing
Promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.

3.9. Principle 9 - Provide support for security incidents

Whilst it is reasonable to expect suppliers to manage security risks in accordance with the contract, you [Supply Chain Owner / Procurement] should be prepared to provide support and assistance if necessary where security incidents have the potential to affect your business or the wider supply chain.

Make requirements clear
You [Supply Chain Owner / Procurement] should clearly set out requirements for managing and reporting security incidents in the contract.

These should clarify supplier's responsibilities for advising you about such incidents - reporting timescales, who to report to etc. Suppliers should also be clear about what support they can expect from you if an incident occurs - required 'clean up' actions, losses incurred, etc.

DPA2018 includes fairly short timescales for telling the Information Commissioner about any incidents, so you and your supply chain need to prepare for this.

Propagate lessons learned
Where lessons have been learnt from security incidents, communicate these to all your suppliers, to help them becoming victims of 'known and manageable' attacks.

Check your arrangements

Businesses will need to gain confidence in their approach to establishing control over their supply chain.

3.10. Principle 10 - Build assurance activities into your supply chain management

- Require those suppliers who are key to the security of your supply chain, via contracts, to provide upward reporting of security performance and to adhere to any risk management policies and processes.
- Build the 'right to audit' into all contracts and exercise this. Require your suppliers to do the same for any contracts that they have let that relate to your contract and your organisation. (Note that this might not always be possible or desirable, particularly where this relates to a Cloud service).
- Build, where justified, assurance requirements such as Cyber Essentials Plus, penetration tests, external audit or formal security certifications into your security requirements.
- Establish key performance indicators to measure the performance of your supply chain security management practice.
- Review and act on any findings and lessons learned.
- Encourage suppliers to promote good security behaviours.

Continuous improvement

As your supply chain evolves, you'll need to continue improving and maintaining security.

3.11. Principle 11 - Encourage the continuous improvement of security within your supply chain

- Encourage suppliers to continue improving their security arrangements, emphasising how this might enable them to compete for and win future contracts with you. This will also help you to grow your supply chain and choice of potential suppliers.
- Advise and support your suppliers as they seek to make these improvements.
- Avoid creating unnecessary barriers to such improvements: acknowledge and be prepared to recognise any existing security practices or certifications they might have that could demonstrate how they meet your minimum security requirements.
- Allow time for your suppliers to achieve security improvements, but require them to provide you with timescales and plans that demonstrate how they intend to achieve them.
- Listen to and act on any concerns highlighted through performance monitoring, incidents, or upward reporting from suppliers that may suggest that current approaches are not working as effectively as planned.

3.12. Principle 12 - Build trust with suppliers

- Seek to build strategic partnerships with key suppliers, sharing issues with them, encouraging and valuing their input. Gain their buy-in to your approach to supply chain security, so that it takes account of their needs as well as your own.
- Let them manage sub-contractors for you, but require them to provide you with appropriate reporting to confirm the status of these relationships.
- Maintain continuous and effective communications with your suppliers.
- Look at supply chain management as a shared issue.