Delegation of authority and Segregation of duties Policy

Brunel University London

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

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	31/07/2018
V 0.2	Andrew Clarke	CISO – clearing definition of what the policy represents, examples of delegation and segregation	07/08/2018
V 1.0	Andrew Clarke	CISA Approval	07/09/2018

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. 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.

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

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London (BUL) covering defining authority to make decisions, including delegation of such authority and requirements for segregation of duties in the organisation required by law or standards in areas such as accounting, corporate governance and information security.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Chief Information Security Officer	Is responsible for monitoring and enforcing the delegation of authority and segregation of duties policy.
All Users	It is the responsibility of all users to read and understand this policy to ensure that, when required, a staff member divides their work among the dependents and give them the responsibility to accomplish the respective tasks and to ensure that the separation (segregation) of duties to prevent fraud and error is adhered to.
Cyber & Information Security Manager	Is responsible for maintaining the delegation of authority and segregation of duties policy and maintaining compliance with ISO27001.
Chief Information Security Officer, Chief Information Officer, Chief Operating Officer, Chief Financial Officer	Review of segregation of duties between critical functions
Chief Procurement Officer	Authorisation for Brunel University toward external parties through signature

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A6 – Organisation of information security

ISO 27001:2013 Conformance Control	Information Classification Objective A.6.1.2 Segregation of duties

1.4 Scope

All employees of Brunel University London.

1.5 Policy Overview

Decision making structures shall be designed with the objective of promoting transparency and placing authority and accountability at appropriate levels of the University. Such structures shall further ensure sound governance, operational efficiency and sufficient segregation of duties in order to prevent fraud and errors.

1.6 Definitions

- Authority is the power or right to make decisions
- Responsibility is a duty or an obligation to perform or complete a task assigned
- Delegation is a transfer of authorisation or responsibility to others

2.0 Delegation of Authority

Delegation of authority is the process of assigning work to another person along with the appropriate level of authority to complete the work. Delegation typically flows from management to their direct and indirect reports. This is a basic management technique that allows for efficiency, resilience and development of team members.

The following are illustrative examples of delegation of authority.

- **1. Function**
  Delegation of an entire organisational function such as an IT Manager who assigns a software developer to be the administrator of a system. This requires the authority to change the system, add users and respond to user inquiries and requests.
- **2. Decision Making**
  Delegation of a decision such as an executive manager who delegates decision making for an office redesign project to a committee of five individuals. In this case, the manager may direct requests to sign off on design decisions to the chairperson of the committee.
- **3. Negotiation**
  A Chief Information Officer grants an IT Manager the authority to negotiate contracts with IT infrastructure partners with final sign off authority remaining with the CIO.
- **4. Strategy**
  The authority to develop and/or implement a strategy. For example, the Marketing Director who delegates a promotional campaign to a marketing officer. This may include authority to manage a team and spend a predefined budget.
- **5. Research & Analysis**
  A mission to research something and return with a report or recommendation. For example, the Director of Commercial Services asks a business analyst to generate a list of large customer accounts that are at risk of cancelling their service. The business analyst states they are acting on behalf of the Director of Commercial Services in requests for the meetings and resources required to complete this request. If meetings or resources are refused, she escalates to the Director of Commercial Services.
- **6. Processes**
  Delegation of a business process. For example, the Head of Development And Application Services who needs to hire 4

software developers delegates the process of short listing candidates to two senior developers.

- **7. Project Sponsorship**
  The Systems Manager sponsors an IS project to improve several systems. The Systems Manager delegates the project sponsor role to a Systems Officer who works with the project team to develop requirements and clear issues. This requires the full authority of the Systems Manager as the Systems Officer may have to overrule objections and push people for decisions and work products.

Delegation, authority and responsibilities

- Brunel University's overall objectives and strategy shall guide delegation making activities
- Job descriptions allocate responsibilities to individuals. The job descriptions detail specific operational responsibilities within the organisational structure and department
- Managers may delegate operational responsibility further through allocation of process and task responsibility, or through allocation of specific actions
- Decisions, including delegations, shall be documented and retained. Documentation requirements depend on the type of decision
- Delegation shall be subject to regular reviews
- Authorisations in Brunel University shall distinguish clearly between internal authority and the power of attorney to commit Brunel University toward external parties through signature, legally binding statements, electronic confirmations and communications or through other means. This responsibility is retained by Procurement

Accountability vs Responsibility

Accountability is the duty to answer for success and failure.
Responsibility is the duty to complete work diligently.
Responsibility can be delegated, accountability **can't** be delegated.
As such, when you delegate something you don't have to do the work but you remain accountable for results.

Effective Delegation

Delegation requires that goals and delegated authority be clearly communicated and agreed to all involved in the work. This is followed by monitoring to step in and help the person doing the

work if it looks like they may fail. At the end, it is helpful to formally or informally assess the results to give the person performance feedback. When work is a success, share the credit. Where it fails, accept accountability.

Delegation vs Setting-Up to Fail

Delegation is normally a way to allow employees to grow into new roles. For example, a manager who delegates management tasks to a senior employee may help that employee to grow into a management position. It is also possible for delegation to end up hurting an individual's career if the assignment is too difficult, goals unclear or if you fail to support them to accomplish the delegated work. This is known as setting the person up to fail.

3.0 Segregation of Duties

Segregation of duties is the principle that no single individual is given authority to execute two conflicting duties. It is a basic type of internal control that is used to manage risk. In many cases, segregation of duties is required by law or standards in areas such as accounting, corporate governance and information security.

Segregation of duties means division or allocation of duties between two or more employees in order to achieve reduced risk for fraud and/or errors

The following are illustrative examples of segregation of duties.

1. **Vendor Maintenance & Posting Invoices**
   Separation of creating vendors in a system from posting and paying invoices. Helps to prevent fictitious customers with fictitious invoices.

2. **Purchase Orders & Approvals**
   Purchase orders typically require multiple approvals.

3. **Payments & Bank Reconciliation**
   Making payments to vendors and reconciliation of bank statements.

4. **Paychecks & Bank Reconciliation**
   Paying employees and bank reconciliation.

5. **Journal Entry & Approvals**
   Separation of entering a journal entry and approval of journal entries.

6. **Custody of Cash & Account Receivable Reconciliation**
   Separating roles that manage cash deposits from customers and reconciliation of those deposits with sales records.

7. **Hire & Set Compensation**
   Hiring an employee and setting their compensation. Helps to prevent people from hiring friends at an inappropriate salary.

8. **Hire & Approve Hire**
   Hiring an employee often has to be approved by multiple departments.

9. **Expenses & Expense Approvals**
   Separation of claiming and approving expenses.

10. **Asset Custody & Asset Inventory**
    Separation of custody of assets and record keeping related to those assets.

11. **Sales & Approvals**
    Separation of selling and approval of sales deals such as approval of margins and customer credit.

12. **Customer Maintenance & Credit Notes**
    Adding customers in a system and posting credit notes.

13. **Shipping & Customer Accounts**
    Shipping and receiving is separated from posting transactions such as credit notes to a customer's account.

14. **Risk Management & Trading**
    Separating risk taking activities such as financial trading from risk management activities.

15. **Advising Clients & Trading**
    Separation of advising banking clients on things such as mergers & acquisition from trading that firm's stock.

16. **Development & Administration**
    Separating development of software and administration of systems, particularly production systems. Allows process to be followed in updating code that is tested and reviewed.

17. **Development & Operations**
    Separation of software development and the operation of related systems and services. Allows problems with software to be reported accurately and managed within process.

18. **System Access Permissions**
    Adding and editing system access permissions is viewed as a root authority that is separated from all financial management activities.

19. **System Configuration & Approvals**

    Changing systems and software typically requires a number of approvals. For example, implementing changes to firewall rules is separated from approving those changes as a basic security control.

The Segregation of duties shall be evaluated by the Department Manager or College Director and implemented for activities where the inherent risk of fraud or errors is significant or critical

The Chief Information Security Officer, Chief Information Officer, Chief Operating Officer and/or Chief Financial Officer may require segregation of duties between functions if deemed necessary from an operational risk perspective. Deviation from the segregation of duties requirements must be approved by the Chief Information Security Officer

Deviations shall be documented, and include a risk acceptance and time limit