Third Party Remote Access Support 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	30/03/2017
V 0.2	Andrew Clarke	References added	05/04/2017
V 0.3	Andrew Clarke	Contractual caveat and Appendix	06/04/2017
V 0.4	Andrew Clarke	PWG technical amendments and exceptions	06/04/2017
V 0.5	Andrew Clarke	Approved CISA	21/04/2017
V 1.0	Andrew Clarke	Approved Information Subcommittee	27/04/2017
V 1.1	Andrew Clarke	Annual review – CISO title change	31/03/2020

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 covering Remote Access for Support purposes by Third Parties.

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
Systems Manager	Is responsible for maintaining and managing systems policies on IT systems and infrastructure and ensuring that third party support complies with this policy.
Network Manager	Is responsible for maintaining and managing network policies on network systems and ensuring that third party support complies with this policy.
Head of Development and Application Services	Is responsible for maintaining and managing password policies on application and web systems and ensuring that third party support complies with this policy.
Cyber & Information Security Manager	Is responsible for maintaining Remote Access policy best practice and ensuring compliance with legislative and regulatory requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A6 – Organization of information security
ISO 27001:2013 Conformance Control	Information Classification Objective A.6.2.2 Teleworking & Remote working security

1.4 Scope

The scope of this policy applies to:

- Brunel University London's contractors, third parties and service providers utilising Brunel University London's information system resources from a remote location;
- Information system resources, including data networks, LAN servers and PC (stand-alone or network-enabled) located on Brunel University London and non-Brunel University London locations, where these systems are under the jurisdiction and/or ownership of Brunel University London, and any personal computers and/or servers authorised to access Brunel University London's data networks;
- Remote access connections used to do work on behalf of Brunel University London, including reading, sending email and viewing intranet web resources from all types of equipment.

1.5 References

CESG Good Practice Guide (GPG) 10 - Remote Working v2.2;
BUL-POL-9.4.3 - Password Policy;
BUL-POL-6.2.1 - Remote Working - Teleworking Policy;
BUL-POL-10.1 - Cryptographic Policy;

1.6 Policy Objectives

The objectives of this policy with regard to the protection of information system resources against unauthorised access from remote locations are to:

- Minimise the threat of accidental, unauthorised or inappropriate access to either electronic or paper-based information owned by Brunel University London or temporarily entrusted to it;
- Minimise Brunel University London's network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources; and
- Minimise reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality.

1.7 Policy Overview

Brunel University London information system resources are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Sufficient precautions are required to prevent and detect unwanted access from unauthorised users in remote locations. Users should be made aware of the dangers of unauthorised remote access, and managers should, where appropriate, introduce special controls to detect or prevent such access

1.8 Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by Brunel University London. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from Brunel

University London intranet (IB) or other relevant communication media on an ongoing basis and accept the terms and conditions contained therein.

2.0 Remote Access Support Policy

2.1 Policy Summary

The purpose of this policy is to protect the confidentiality, integrity and availability of Brunel University London's information by controlling remote access to University information Services (IS) systems by third parties in support of IS systems and to define standards for connecting to Brunel University London's network from third party hosts.

Brunel University London's IS resources are assets important to Brunel University London's business and stakeholders and its dependency on these assets demands that appropriate levels of IS be instituted and maintained. It is Brunel University London's policy that appropriate remote access control measures are implemented to protect its IS resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such IS resources.

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration between the University and third parties, they also provide a back door into the University network that can be used for theft of, unauthorised access to, or destruction of assets.
All remote access tools used to communicate between Brunel University London assets and other systems must comply with the following policy requirements

3.0 Method Statement

The purpose of this policy is to set out governing principles that apply to the cyber and information security of Brunel University in regard to third party remote access. However, contractual obligations specifically identified and documented within the contract, can supersede these policy dictates in the relevant areas.

Privileged access by third parties to University data or systems should be approved by the Head of Department responsible for the data or system. The Head of Department must also name the member of University staff who will manage access by the third party;

The third party must specify which members of its staff will be involved in handling or accessing the University's IT systems. The number of staff involved must be kept to a minimum necessary to deliver the service;

Access must only be given to the minimum set of data required for the third party to fulfil their contract. Test, dummy or sample data must be used unless there is compelling reason not to do so;

A member of University staff, named by the Head of Department, must be responsible for managing the access provided in terms of scope, level and duration and must ensure the activities of the third party are monitored in person and logged either electronically or manually. If individual monitoring is unwarranted, monitoring is permitted via firewall holes;

Privileged remote access must support strong, end-to-end encryption of the remote access communication channels from nominated remote (IP) addresses for the minimum required amount of time as specified in the Brunel University London network encryption protocols policy;

All remote access tools or systems that allow communication to Brunel University London resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password;

Changes made by a third party organisation to a University IS Service or live environment must follow the same change management procedure that would apply if those changes were being made by University staff;

Third parties are prohibited from installing software on the University's client computer without prior consent and have to follow the University change management procedure to enact changes before deployment;

If a third party makes use of a privileged account access must be removed as soon as the work is complete;

Any data transferred to the third party must be either returned or destroyed when specified by the agreed service contract;

The third party must immediately notify the University of any Information Security Incidents which might impact on its service to the University or affect the security or confidentiality of any University data;

Third party access arrangements must be reviewed on an annual basis to ensure information security risks are being managed effectively and to validate that access is still required. Evidence of the review should be retained by the Head of Department for three years;

The authentication database source must be Active Directory or LDAP, or via guest VPN access to local server accounts that have no domain wide access and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session;

Remote access tools must support the Brunel University London application layer proxy rather than direct connections through the perimeter firewall(s);

All Brunel University London antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way;

If the access involves transfer of personal data outside the European Economic Area the access is to be governed by a contract which provides for the transfer and security of the data under the seventh and eighth Data Protection principles;

For any third party access, the University and third party must agree in advance a code of practice and non-disclosure agreement to protect University information and working practices;

Brunel University London's information system resources shall be appropriately protected to prevent unauthorised remote access;

The further sharing of screens with additional parties without University consent is prohibited;

Compliance with other Brunel University London policies must be adhered to, in particular BUL-POL-9.4.3 - Password Policy, BUL-POL-6.2.1 - Information Security Remote Working Policy, and BUL-POL-10.1 - Cryptographic Policy and the Brunel Acceptable Computer Use Policy (BACUP);

<PAGE LEFT DELIBERATELY BLANK>

APPENDIX A – Third Party Agreement on IS Remote Access

THIRD PARTY INFORMATION SERVICES REMOTE ACCESS AGREEMENT

This third party agreement (the "**Agreement**") is made and entered into as of *[DATE OF AGREEMENT]* (the "**Effective Date**") between Brunel University London (the "**University)**, and *[NAME OF THIRD PARTY] (*the "**Contractor**") (collectively, the "**Parties**").

The University requests the Contractor to perform services for it; and

The Contractor therefore agrees as follows:

1.0. **Term and Termination**.

1.1. This Agreement takes effect immediately as of the Effective Date, and remains in full force and effect until the Contractor has completed the Services (the "**Term**"), unless earlier terminated.

1.2. The University may terminate the Contract for cause by providing the Contractor written notice if the Contractor is in material breach of this Agreement and has failed to cure such breach within five (5) days after its receipt of written notice of such breach provided by the University.

2.0. Contractor Agreement.

2.1 The Contractor (and all of its subcontractors, employees or representatives, or agents of any kind) agrees to comply with the following University Policies:

- BUL-POL-6.2.2 – Third Party Remote Access Support Policy;
- BUL-POL-9.4.3 - Password Policy,
- BUL-POL-6.2.1 – Information Security Remote Working Policy;
- BUL-POL-10.1 - Cryptographic Policy;
- Brunel Acceptable Computer Use Policy (BACUP);

3.0. University Confidential Information.

3.1 The Contractor (on its behalf and on behalf of its subcontractors, employees or representatives, or agents of any kind) agrees to treat all University Confidential information of the University, including, but not limited to, Research, Financial, Personal Identifiable information and any other information that the Third Party reasonably should know is confidential ("**University Confidential Information**") as confidential and protect the University Confidential Information with the same degree of care as used to protect its own Confidential Information of like nature.

4.0 Miscellaneous Provisions.

4.1. This Agreement constitutes the agreement between the Parties with respect to the subject matter of this Agreement, and supersedes all prior negotiations,

agreements, representations, and understandings of any kind, whether written or oral, between the Parties, preceding the date of this Agreement.

4.2. This Agreement may be amended only by written agreement duly executed by an authorised representative of each party (email is acceptable).

4.3. If any provision or provisions of this Agreement shall be held unenforceable for any reason, then such provision shall be modified to reflect the parties' intention. All remaining provisions of this Agreement shall remain in full force and effect for the duration of this Agreement.

The Parties are signing this Agreement on the date stated in the introductory clause.

BRUNEL UNIVERSITY LONDON

By: _____

Name:

Title:

THIRD PARTY NAME

By:_____

Name:

Title: