REMOTE ACCESS

POLICY DOCUMENT

Document Id	Remote Access Policy
Sponsor	Laura Gibbs
Author	Nigel Rata
Date	May 2014

Version Control Log

Version	Date	Change
1.0	15/05/12	Initial draft for review
1.1	15/05/2014	Annual Update

Document Approval

Name	Approval Signature	Approval Date
ITUAG	Approved	27.5.14

Introduction and Scope

This policy applies to all University employees, students, and affiliates including vendors and agents with a university owned or personally-owned computer or workstation used to connect to the RHUL network. This policy applies to remote access connections used to do work on behalf of RHUL or for personal business, including reading or sending email and viewing intranet web resources.

Purpose

The purpose of this policy is to define standards for connecting to the RHUL network from any remote host. These standards are designed to minimize the potential exposure to the University from damages which may result from unauthorized use of university resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

Policy

RHUL hosts numerous services that can be contacted from the public internet. These can be open access e.g. college main website or require user authentication (such as student portal or e-mail system etc.). Some of the resources available to RHUL staff are not available from the public internet (such as access to some cooperate systems or desktop computers).

RHUL provides a method for connecting remote hosts to our network. We utilise VPN (Virtual Public Network) technology which allows authenticated individuals to access services that are blocked at the RHUL perimeter firewall or internal firewall level.

This policy outlines who can have access to this remote access solution and outlines any exceptions to the standard policy.

By default all valid RHUL usernames have access to the VPN service. Users without a valid username and password cannot authenticate on this service and cannot gain access via this remote access service.

Please refer to the 3rd party access policy for expanded rules around the use of remote access for 3rd parties.

In certain cases RHUL IT services may need to block access or terminate connections made through the remote access service. This is usually as a response to security incident or infringements of the RHUL or JANET acceptable use policy. In these cases access may be blocked and the user informed by e-mail of the blockage and any details relevant to the situation. Access would be granted again once the situation has been resolved satisfactorily.

This policy will be reviewed annually.