Remote Access and Bring Your Own Device Policy (BYOD)

Version: 1.0
Date: 24th May 2018
Author: MRC Print Limited

Remote Access Policy

What is Remote Access

Remote access refers to technology that enables you to connect users in geographically dispersed locations. This access is typically over some kind of dial-up connection, although it may include Wide Area Network (WAN) connections. These connections represent a security risk to MRC Print Limited and as such need to be carefully managed.

Purpose

The purpose of this policy is to define rules and requirements for connecting to MRC Print Limited network from any host. These rules and requirements are designed to minimise the potential exposure to MRC Print Limited from damages that may result from unauthorised use of MRC Print Limited resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical MRC Print Limited internal systems and fines or other financial liabilities incurred as a result of those losses.

Scope

The policy covers all types of remote access, whether fixed or 'roving' including

- Travelling users (e.g. staff working across sites or temporarily based at other locations)
- Home workers
- Non practice staff (e.g. contractors and other third party organisations)
- All other remote access means

Objectives

The objectives of the company's policy on remote access by staff are

- To provide secure and resilient remote access to the company's information systems
- To preserve the integrity, availability and confidentiality of the company's data and information systems
- To manage the risk of serious financial loss, a loss of client confidence or other serious business impact which may result from a failure in security
- To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the company is adequately protected under computer misuse legislation

Responsibilities

- MRC Print Limited is ultimately responsible for ensuring that remote access by staff is managed securely
- The company will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks
- The company is responsible for confirming whether remote access to business applications and systems is permitted
- The data protection officer is responsible for providing authorisation for all remote access users and the level of access provided
- The data protection officer will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels
- The data protection officer will provide assistance on implementing controls
- The data protection officer is responsible for assessing risks and ensuring that controls are being applied effectively
- All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify the data protection officer immediately of any security incidents and breaches
- Users must return all relevant equipment on termination of the need to use remote access

Risk

The practice recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example

- Unavailability of network, systems or target information
- Degraded performance of remote connections
- Loss or corruption of sensitive data
- Breach of confidentiality
- Loss of or damage to equipment
- Breach of legislation or non-compliance with regulatory or ethical standards

Security Architecture

The security architecture is typically integrated into the existing company network and is dependant on the IT services that are offered through the network infrastructure. These Include

- Password authentication, authorisation and accounting
- Strong authentication
- Security monitoring by intrusion detection systems

User Identity

All remote users must be registered and authorised by the I.T Department. User identity will be confirmed by strong password/ user I.D authentication. The data protection officer is responsible for ensuring a log is kept of all user remote access.

Perimeter Security

The data protection officer will be responsible for ensuring perimeter security devices are in place and operating normally. Perimeter security solutions control access to critical network applications, data and services, so that only legitimate users and information can pass through the network. Complementary tools, including virus scanners and content filters, also help control network perimeters. Firewalls are generally the first security products that organisations deploy to improve their security postures.

Secure Connectivity

The company will protect confidential information from eavesdropping or tampering during transmission.

Security Monitoring

Network vulnerability scanners will be used to identify areas of weakness, and intrusion detection systems will monitor, and reactively respond to, security events as they occur.

System Change Control

All changes to systems must be recorded on a system change control form and authorised by the I.T Department.

Reporting Security Incidents & Weaknesses

All security weaknesses and incidents must be reported to the data protection officer.

Guidelines and training

The data protection officer will produce written guidance and training materials for all remote access users.

Bring Your Own Device Policy

Introduction

This policy provides policies, standards, and rules of behaviour for the use of personally owned smart phones and/or tablets by MRC Print Limited employees who access MRC Print Limited network resources. Access to and continued use of network services is granted on condition that each user reads, signs, respects and follows the MRC Print Limited policies concerning the use of these devices and services.

Expectation of Privacy

MRC Print Limited will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads company email/attachments/documents to their personal device). This differs from policy for company provided equipment/services, where company employees do not have the right, nor should they have the expectation of, privacy while using company equipment or services.

Requirements

In order to allow employees to access MRC Print Limited resources on their own devices it is important that these devices are secure. This includes

- User will not download or transfer sensitive business data to their personal devices
- User will password protect the device
- User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer
- The user will not “jailbreak” the device (installing software that allows the user to bypass standard built-in security features and controls)
- User agrees that the device will not be shared with other individuals or family members, due to the business use of the device (potential access to company email etc)
- User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments

Risk

While IT will take every precaution to prevent the employee’s personal data from being lost; in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts etc. In addition:

- The company reserves the right to disconnect devices or disable services without notification

- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above
- The employee is personally liable for all costs associated with his or her device
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures or programming errors that render the device unusable
- The company reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy

To this extent MRC Print Limited should ensure all users sign an appropriate agreement.

Validity Of This Policy

This policy should be reviewed regularly under the authority of the data protection officer. Associated information and security standards should be subject to an on going development and review programme.

End of document.