RATP Dev UK Ltd and its subsidiaries ("RDUK Group")*

Information Systems Security Policy

Prepared By:	**Robin Newby**
Department:	**I.T. Systems**
Created:	**26 Jan 2004 13:39:00**
Last Revision Date:	**23 May 2018 09:51:00**
Version	**2.0**

*Excluding The Original Tour Ltd

1. Introduction

Data is crucial to the successful operation and delivery of services by RDUK Group and so is the handling and security, which surrounds it. The integrity, accuracy, and availability of information systems underpin the operations of RDUK Group.

Failure to secure RDUK Group information systems and the data that they contain, will jeopardise the ability of RDUK Group to fulfil the delivery of transportation services, and could potentially have greater long-term impact through the consequential risk of financial or reputational loss.

This Information Systems Security policy outlines the principles and responsibilities of users of RDUK Group's information systems required to safeguard them and the data that they contain.

The IT department are crucial in helping the companies' successfully implement information security management, but this will only be possible if all staff of RDUK Group are aware of, and carry out their own personal responsibilities.

2. The scope, aims and awareness

2.1 Policy Scope

The Information Systems Security Policy applies to all staff of RDUK Group, and third parties accessing the companies' systems or data.

2.2 Policy Aims

1. Ensure the protection of Information Systems from security threats, and reduce and mitigate risks.

2. Ensure that all users are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access.

3. Safeguard the reputation and business of RD UK by ensuring its ability to meets its legal obligations; and to protect it from liability or damage through misuse of its IT services or data.

2.3 Policy awareness and communication

All users are to be provided with this policy immediately upon issue, and any new users upon the creation and provision of their account. Any updates to this policy and further guidance provisioned via local Intranets.

2.4 Policy Review

This policy will be reviewed annually or when required to ensure that it remains appropriate and up to date. Any questions or concerns should be raised with the Head of Information Systems.

3. Information security principles

The following principles provide a framework for the security and management of RDUK Group information and information systems.

1. Where personal data are stored, appropriate consent for storage and processing must be gathered and recorded.
2. All individuals covered by the scope of this policy must handle information appropriately.
3. Information will only be available to those with a legitimate need for access.
4. Information will be protected against unauthorised access and processing.
5. Information will be protected against loss and corruption.
6. Security countermeasures, both electronic and physical deployed to protect and secure systems and data contained within them.
7. Information will be disposed of securely and in a timely manner.
8. Breaches of policy must be reported by anyone aware of the breach in a timely manner.

4. Compliance and Incident notification

It is vital that all users of information systems of RDUK Group and its subsidiaries comply with the information security policy.

Any breach of information security is a serious matter and could lead to the possible loss of personal or other confidential data. Such a loss may result in criminal or civil action against the RDUK Group and the loss of business and financial penalties.

Any actual or suspected breach of this policy must be notified to the Head of Information Systems or the IT Manager at the earliest possible opportunity.

5. Responsibilities

5.1 Users

Users must adhere to the Acceptable Use Policy and other relevant policies and supporting procedures and guidance. A user should only access systems and information where they have a legitimate need and must not knowingly attempt to gain access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data.

5.2 Systems and Data Administrators and super users

Systems and Data administrators are responsible for the information systems that hold data and access to it. In addition to their individual responsibilities 4.1, they must:

- Ensure that the physical and network security of systems is maintained.
- Ensure that the systems they maintain are suitably configured and maintained.
- Ensure that the data is appropriately stored and backed up.
- Adhere to change controls surrounding data access, security access, and programmatic upgrades and modifications.
- Ensure that appropriate access controls are in place.
- Understand and document risks, taking suitable steps to mitigate whilst ensuring that data owners understand them.
- Document operational procedures and responsibilities of staff.
- Publish procedures for users of the systems to allow secure access and usage.
- Ensure that systems are compliant with legal and other contractual requirements.

5.3 Password security

Password security is in place across the group to ensure complexity and their regular change is enforced. Failure to follow this policy results in accounts automatic lockout. Passwords and accounts must not be shared amongst users.

5.4 Workstation security

Users are responsible for ensuring the security of their workstation; and should lock it when away from their desks. An automatic screen lock procedure ensures that a workstation will lock out after a set number of minutes of inactivity.

5.5 Laptop security

Laptop hard drives are encrypted to ensure that data is secure should the device be lost, stolen, or the hard drive is removed.

5.6 IT Department

The IT Department must ensure that the provision of IT infrastructure is consistent with the demands of this policy.