Information Security Policy

TRL is committed to maintaining and continually improving an Information Security Management System (ISMS) that satisfies applicable requirements and is certified to the international standard ISO/IEC 27001:2013. This Policy provides the top level organisational intention for the management of Information security and the associated risks and identifies the core structure through which effective information security will be implemented and maintained.

All employees, regardless of their role, are responsible for conducting their work in a manner that protects the security of TRL's information assets.

This policy will be supported by and implemented through the ISMS and its associated policies and procedures. The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by TRL within which:

- All members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation;
- Adequate resources are made available to support the ISMS;
- Information assets under the control of TRL are adequately protected against unauthorised access, deliberate or unintentional corruption, loss or deletion;
- Information assets and the supporting business processes, systems and applications, will be protected by implementing appropriate controls to preserve their confidentiality, integrity and availability;
- Risks to information assets will be actively identified and assessed to identify controls that reduce risks to an acceptable level;
- Confidentiality of information is protected; appropriate to its sensitivity;
- Third parties with access to information assets under the control of TRL will be assessed to ensure they meet the necessary information security requirements;
- Business continuity plans are in place and will be tested periodically;
- Legislative, regulatory or contractual requirements appropriate to TRL's business are identified and met;
- Actual or suspected information security breaches are identified, analysed and investigated;
- Information security objectives are monitored and reviewed annually at the Management Review Meeting;
- The effectiveness of the ISMS is continually improved.

This policy has immediate effect and replaces all previous versions. It will be reviewed annually or sooner should a significant change occur in order to ensure its continuing suitability, adequacy and effectiveness.

The policy will be communicated within TRL and made available to interested parties.

Rob Wallis
Chief Executive
TRL