SPARK TSL POLICY DOCUMENT

Quality and Information Security Policy Statement

Document Owner	Jane Stephenson
Version	1.5

Contents

1. Intent and purpose

This Policy sets out SPARK Technology Services Limited top-level intent, principles and commitments for Quality, Environmental Management, Information Security and Privacy.

It is appropriate to our purpose and context, aligns with our strategic direction, and provides the framework for establishing and reviewing objectives. It demonstrates top management's commitment to satisfy applicable requirements and to the continual improvement of our Integrated Management System (IMS).

2. Policy

2.1. Quality Commitments (ISO 9001:2015)

- Ensure the Quality Policy is appropriate to the purpose and context of SPARK and supports the organisation's strategic direction.
- Provide a framework for setting and reviewing measurable quality objectives that drive customer satisfaction and process effectiveness.
- Meet or exceed customer, statutory and regulatory requirements.
- Ensure competent people, effective processes and suitable resources are available to fulfil requirements.
- Use risk-based thinking and evidence to improve products, services and the effectiveness of the Quality Management System (QMS).
- Make this Policy available as documented information and, as appropriate, to relevant interested parties.

2.2. Information Security Commitments (ISO/IEC 27001:2022)

- Preserve the confidentiality, integrity and availability of information and systems via a risk-based Information Security Management System (ISMS).
- Ensure this Policy is appropriate to the organisation's purpose, risk environment and stakeholder requirements.
- Provide a framework for setting and reviewing information security objectives aligned to business needs.
- Satisfy applicable legal, regulatory and contractual information security requirements and other obligations.
- Assign and communicate information security roles, responsibilities and authorities; top management provides direction and support for information security.
- Continually improve the ISMS through monitoring, measurement, internal audit and management review.

2.3. Privacy Commitments (ISO/IEC 27701 – PIMS)

Where we act as a controller and/or processor of personally identifiable information (PII), we establish and maintain a Privacy Information Management System (PIMS) integrated with the IMS. We commit to:

- Determine and document SPARK's role (controller, joint controller, or processor) for each PII processing activity.
- Process PII lawfully, fairly and transparently for specified, explicit and legitimate purposes; apply data minimisation, accuracy, storage limitation, and integrity/confidentiality.
- Define privacy roles and responsibilities, including those of senior leadership and, where appointed, the Data Protection Officer (DPO).
- Respect data subject rights (e.g., access, rectification, erasure, restriction, objection and portability) and respond within statutory timeframes.
- Assess and manage privacy risks (including Data Protection Impact Assessments where required) and embed privacy by design and by default into products and services.
- Maintain records of processing activities, lawful bases, retention schedules and international data transfer mechanisms.
- Establish incident and breach response procedures, including notification to authorities and affected individuals where legally required (e.g., UK GDPR / DPA 2018).
- Set and review privacy objectives and continually improve the effectiveness of the PIMS.

2.4. Environmental Commitments (ISO 14001:2015)

- Protect the environment, including the prevention of pollution and other commitments relevant to our context (e.g., sustainable resource use, climate change mitigation and adaptation, and protection of biodiversity and ecosystems).
- Fulfil compliance obligations and other requirements related to our environmental aspects and impacts.
- Minimise waste and energy consumption; promote reuse and recycling; manage hazardous substances responsibly.
- Provide a framework for setting environmental objectives and continually improve the Environmental Management System (EMS) to enhance environmental performance.

2.5. Healthcare-specific Commitments (NEN 7510 / Dutch Healthcare Laws)

- Apply heightened safeguards to personal health information (PHI) processed for healthcare customers, in addition to general PII controls.
- Ensure unique identification of healthcare recipients within health information systems and validate health data outputs in accordance with care-specific controls.
- Maintain complete and tamper-resistant logging of access to PHI and retain such logs per legal and contractual requirements.
- Isolate PHI-processing environments from unrelated infrastructure, enforce least privilege, and apply strong authentication appropriate to risk.
- Comply with applicable Dutch healthcare legislation

2.6. Communication, Availability & Control of the Policy

This Policy is controlled as documented information, communicated to persons working for or on behalf of the organisation, and made available to relevant interested parties. The latest approved version is published on the company intranet and, where appropriate, externally.

2.7. Objectives & Measurement

Measurable quality, environmental, information security and privacy objectives will be defined, monitored and reviewed at planned intervals. Performance is tracked via KPIs, audits, risk assessments and corrective actions.

2.8. Review & Continual Improvement

This Policy and the IMS are reviewed at least annually and after significant changes or incidents to ensure continuing suitability, adequacy and effectiveness. Opportunities for improvement are recorded and implemented.

3. Scope

This Policy applies to all activities, people and information systems used to deliver the provision of design, development, installation, repair and management solutions for Wi-Fi, patient entertainment and engagement systems, and supporting software services to national and international clients. Unless stated otherwise, the scope includes on-premises and cloud environments, products and services we operate or manage, and third parties acting on our behalf.

4. Roles, Responsibilities & Awareness

- Top Management: approves this Policy, ensures resources, sets direction, and reviews IMS performance.
- Information Security Lead/ISMS Owner: maintains the ISMS/PIMS, monitors performance, reports to management.
- Quality/Environmental Leads: maintain the QMS/EMS and coordinate objectives and compliance.
- All Employees and Contractors: follow policies and procedures, complete required training, and report incidents or nonconformities promptly.

Approved by:	Name:	Date:
Signed: 	Jane Stephenson – CEO	23/01/2026