1 ISMS Policy

1.1 Information Security Requirements

A clear definition of the requirements for information security will be agreed and maintained with the business so that all ISMS activity is focused on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements regarding the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the **CITIBILL** A.E. Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

1.2 Top Management Leadership and Commitment

Commitment to information security extends to senior levels of the organization and will be demonstrated through this ISMS Policy and the provision of appropriate resources to provide and develop the ISMS and associated controls.

Top management will also ensure that a systematic review of performance of the program is conducted on a regular basis to ensure that quality objectives are being met and relevant issues are identified through the audit program and management processes. Management review can take several forms including departmental and other management meetings.

The **Information Security Manager** shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

- The identification, documentation and fulfilment of information security requirements
- Implementation, management and improvement of risk management processes
- Integration of operational processes, procedures and controls
- Compliance with statutory, regulatory and contractual requirements
- Reporting to top management on performance and improvement

1.3 Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

ISMS objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001:2013 the reference controls detailed in Annex A of the standard will be adopted where appropriate by **CITIBILL** A.E.. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

1.4 Roles and Responsibilities

Within the field of information security, there are a number of management roles that correspond to the areas defined within the scope set out above. In a larger organization, these roles will often be filled by an individual in each area. In a smaller organization these roles and responsibilities must be allocated between the members of the team.

Full details of the responsibilities associated with each of the roles and how they are allocated within **CITIBILL** A.E. are given in a separate document *Information Security Roles, Responsibilities and Authorities*.

It is the responsibility of the **Information Security Manager** to ensure that employees and contractors understand the roles they are fulfilling and that they have appropriate skills and competence to do so.

1.5 Continual Improvement of the ISMS

CITIBILL A.E. policy with regard to continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings with interested parties and document them in a continual improvement plan
- Review the continual improvement plan at regular management meetings in order to prioritize and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be added to the continual improvement plan and evaluated by the staff member responsible for continual service improvement.

As part of the evaluation of proposed improvements, the following criteria will be used:

- Cost
- Business Benefit
- Risk
- Implementation timescale
- Resource requirement

If accepted, the improvement proposal will be prioritized in order to allow more effective planning.

1.6 Approach to Managing Risk

Risk management will take place at several levels within the ISMS, including:

- Management planning – risks to the achievement of information security objectives will be assessed and reviewed on a regular basis
- Information security and IT service continuity risk assessments
- Assessment of the risk of changes via the change management process
- As part of major projects to achieve business change e.g. new computer systems

High level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision.

A risk assessment process will be used which is line with the requirements and recommendations of ISO/IEC 27001, the International Standard for Information Security. This is documented in *Risk Assessment and Treatment Process*.

From this analysis, a risk assessment report will be generated followed by a risk treatment plan in which appropriate controls will be selected from the reference list in Annex A of the ISO/IEC 27001 standard, together with any additional controls thought to be necessary.

1.7 Human Resources

CITIBILL A.E. will ensure that all staff involved in information security are competent on the basis of appropriate education, training, skills and experience.

The skills required will be determined and reviewed on a regular basis together with an assessment of existing skill levels within **CITIBILL** A.E.. Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place.

Training, education and other relevant records will be kept by the HR Department to document individual skill levels attained.

1.8 Auditing and Review

Once in place, it is vital that regular reviews take place of how well information security processes and procedures are being adhered to. This will happen at three levels:

1. Structured regular management review of conformity to policies and procedures
2. Internal audit reviews against the ISO/IEC 27001 standard by the **CITIBILL** A.E. Quality Team
3. External audit against the standard by a Registered Certification Body (RCB) in order to gain and maintain certification

Details of how internal audits will be carried out can be found in *Procedure for ISMS Audits*.

1.9 Documentation Structure and Policy

All information security policies and plans must be documented. Details of documentation conventions and standards are given in the *Procedure for the Control of Documented Information*.

A number of core documents will be maintained as part of the ISMS. They are uniquely numbered, and the current versions are tracked in the *ISMS Documentation Log*.

1.10 Control of Records

The keeping of records is a fundamental part of the ISMS. Records are key information resources and represent evidence that processes are being carried out effectively.

The controls in place to manage records are defined in the document *Procedure for the Control of Documented Information*.