

**Circle FinTech Ltd.**

**Statement of Applicability**

|  |  |
| --- | --- |
| Code: | CISMS/IT/ISO/6 |
| Version: | 1.0 |
| Date of version: | 27th March 2018 |
| Prepared for: | A partial fulfilment of ISO/IEC-27001 |
| Created by: | SHAHAB AL YAMIN CHAWDHURY |
| Approved by: | Redwan-ul Karim Ansari |
| Confidentiality level: | HIGH |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 2018-03-27 | 1.0 | Shahab Al Yamin Chawdhury | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415649225)

[2. Reference documents 3](#_Toc415649226)

[3. Applicability of controls 3](#_Toc415649227)

[4. Acceptance of Residual Risks 21](#_Toc415649228)

[5. Validity and document management 22](#_Toc415649229)

# Purpose, scope and users

The purpose of this document is to define which controls are appropriate to be implemented in Circle FinTech Ltd., the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information Security Management System (ISMS) scope.

Users of this document are all employees of Circle FinTech Ltd., who have a role in the ISMS.

# Reference documents

* ISO/IEC 27001 standard, clause 6.1.3 d)
* Information Security Policy
* Risk Assessment and Risk Treatment Methodology
* Risk Assessment and Risk Treatment Report

# Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Controls according to ISO/IEC 27001 | Applicability (YES/NO) | Justification for selection/ non-selection | Control objectives | Implementation method | Status |
| A.5 | Information security policies | YES | ISMS Enforcement | ISO/IEC 27001 | Software & Hardware | Implementation ongoing |
| A.5.1 | Management direction for information security | YES | ISMS Enforcement | Control objectives | Software & Hardware | Approved Implementation |
| A.5.1.1 | Policies for information  security | YES | ISMS Enforcement | ISO/IEC 27001 | All policies referred to below in this column | Implementation ongoing |
| A.5.1.2 | Review of the policies  for information  security | YES | ISMS Enforcement | Control objectives | Each policy has a designated owner who has to review the document at planned interval |  |
| A.6 | Organization of information security | YES | ISMS Enforcement | ISO/IEC 27001 |  |  |
| A.6.1 | Internal organization | YES | ISMS Enforcement | Control objectives |  |  |
| A.6.1.1 | Information security  roles and responsibilities | YES | ISMS Enforcement | ISO/IEC 27001 | Responsibilities for information security are listed in various ISMS documents. If required, IT Dept. Head defines additional responsibilities |  |
| A.6.1.2 | Segregation of duties | YES | ISMS Enforcement | Control objectives | Any activity that includes sensitive information is approved by one person and implemented by another |  |
| A.6.1.3 | Contact with authorities | YES | ISMS Enforcement | ISO/IEC 27001 | Business Continuity Strategy, Incident Response Plan |  |
| A.6.1.4 | Contact with special  interest groups | YES | ISMS Enforcement | Control objectives | IT Dept. Head is responsible for monitoring |  |
| A.6.1.5 | Information security  in project management | YES | ISMS Enforcement | ISO/IEC 27001 | Project manager is required to include applicable information security rules in every project, this also could lead by the IT Dept. Head |  |
| A.6.2 | Mobile devices and teleworking | YES | ISMS Enforcement | Control objectives | BYOD |  |
| A.6.2.1 | Mobile device policy | YES | ISMS Enforcement | ISO/IEC 27001 | Acceptable Use Policy / Mobile Device and Teleworking Policy, Bring Your Own Device (BYOD) Policy |  |
| A.6.2.2 | Teleworking | YES | ISMS Enforcement | Control objectives | Acceptable Use Policy / Mobile Device and Teleworking Policy |  |
| A.7 | Human resource security | YES | ISMS Enforcement | ISO/IEC 27001 | HR |  |
| A.7.1 | Prior to employment | YES | ISMS Enforcement | Control objectives | HR |  |
| A.7.1.1 | Screening | YES | ISMS Enforcement | ISO/IEC 27001 | HR Dept. Head checks each candidate by any method for verification checks – e.g. checking the CV, contacting former employers, checking criminal records, financial status, etc.; [Supplier Security Policy - Exclusion] |  |
| A.7.1.2 | Terms and conditions  of employment | YES | ISMS Enforcement | Control objectives | HR Control |  |
| A.7.2 | During employment | YES | ISMS Enforcement | ISO/IEC 27001 | HR Control |  |
| A.7.2.1 | Management responsibilities | YES | ISMS Enforcement | Control objectives | Management actively requires that all ISMS rules be implemented by all employees, suppliers and outsourcing partners |  |
| A.7.2.2 | Information security  awareness, education  and training | YES | ISMS Enforcement | ISO/IEC 27001 | Information Security Policy, Training and Awareness Plan, [Supplier Security Policy - Exclusion] |  |
| A.7.2.3 | Disciplinary process | YES | ISMS Enforcement | Control objectives | Incident Management Procedure, Statement of Acceptance of ISMS Documents |  |
| A.7.3 | Termination and change of employment | YES | ISMS Enforcement | ISO/IEC 27001 | HR |  |
| A.7.3.1 | Termination or change  of employment responsibilities | YES | ISMS Enforcement | Control objectives | All agreements with suppliers and partners contain clauses that remain valid after the termination of employment, as well as the Confidentiality Statements, signed with employees. |  |
| A.8 | Asset management | YES | ISMS Enforcement | ISO/IEC 27001 | Inventory of Assets |  |
| A.8.1 | Responsibility for assets | YES | ISMS Enforcement | Control objectives | Inventory of Assets, Information Classification Policy |  |
| A.8.1.1 | Inventory of assets | YES | ISMS Enforcement | ISO/IEC 27001 | Inventory of Assets, Information Classification Policy |  |
| A.8.1.2 | Ownership of assets | YES | ISMS Enforcement | Control objectives | Inventory of Assets, Acceptable Use Policy |  |
| A.8.1.3 | Acceptable use of  assets | YES | ISMS Enforcement | ISO/IEC 27001 | Acceptable Use Policy |  |
| A.8.1.4 | Return of assets | YES | ISMS Enforcement | Control objectives | Acceptable Use Policy; Supplier Security Policy |  |
| A.8.2 | Information classification | YES | ISMS Enforcement | ISO/IEC 27001 |  |  |
| A.8.2.1 | Classification of information | YES | ISMS Enforcement | Control objectives | Information Classification Policy |  |
| A.8.2.2 | Labeling of information | YES | ISMS Enforcement | ISO/IEC 27001 | Information Classification Policy |  |
| A.8.2.3 | Handling of assets | YES | ISMS Enforcement | Control objectives | Information Classification Policy |  |
| A.8.3 | Media handling | YES | ISMS Enforcement | ISO/IEC 27001 | Information Classification Policy, PR |  |
| A.8.3.1 | Management of removable  media | YES | ISMS Enforcement | Control objectives | Information Classification Policy |  |
| A.8.3.2 | Disposal of media | YES | ISMS Enforcement | ISO/IEC 27001 | Operating Procedures for Information and Communication Technology / Disposal and Destruction Policy |  |
| A.8.3.3 | Physical media transfer | YES | ISMS Enforcement | Control objectives | Information Classification Policy |  |
| A.9 | Access control | YES | ISMS Enforcement | ISO/IEC 27001 | Physical & Server HW & SW, Acceptable use Policy |  |
| A.9.1 | Business requirements of access control | YES | ISMS Enforcement | Control objectives | Acceptable use Policy |  |
| A.9.1.1 | Access control policy | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy |  |
| A.9.1.2 | Access to networks and network services | YES | ISMS Enforcement | Control objectives | Access Control Policy |  |
| A.9.2 | User access management | YES | ISMS Enforcement | ISO/IEC 27001 |  |  |
| A.9.2.1 | User registration and  de-registration | YES | ISMS Enforcement | Control objectives | Access Control Policy] / Password Policy |  |
| A.9.2.2 | User access provisioning | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy] / Password Policy |  |
| A.9.2.3 | Management of privileged  access rights | YES | ISMS Enforcement | Control objectives | Access Control Policy |  |
| A.9.2.4 | Management of secret  authentication information  of users | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy / Password Policy |  |
| A.9.2.5 | Review of user access  rights | YES | ISMS Enforcement | Control objectives | Access Control Policy |  |
| A.9.2.6 | Removal or adjustment  of access rights | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy |  |
| A.9.3 | User responsibilities | YES | ISMS Enforcement | Control objectives | Acceptable Use Policy, Access Control Policy / Password Policy |  |
| A.9.3.1 | Use of secret authentication  information | YES | ISMS Enforcement | ISO/IEC 27001 | Acceptable Use Policy, Access Control Policy / Password Policy |  |
| A.9.4 | System and application access control | YES | ISMS Enforcement | Control objectives | Acceptable Use Policy, Access Control Policy / Password Policy |  |
| A.9.4.1 | Information access  restriction | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy, Information Classification Policy |  |
| A.9.4.2 | Secure log-on procedures | YES | ISMS Enforcement | Control objectives | A secure log-on process exists for all computers on the network |  |
| A.9.4.3 | Password management  system | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy / Password Policy |  |
| A.9.4.4 | Use of privileged utility  programs | YES | ISMS Enforcement | Control objectives | Only [HoIT] has the right to use privileged utility programs |  |
| A.9.4.5 | Access control to program  source code | YES | ISMS Enforcement | ISO/IEC 27001 | The program source code is stored [describe technical implementation and only IT Dept. Head and Dev. Dep.t Head has access rights |  |
| A.10 | Cryptography | YES | ISMS Enforcement | Control objectives | Policy on the Use of Cryptographic Controls |  |
| A.10.1 | Cryptographic controls | YES | ISMS Enforcement | ISO/IEC 27001 | Policy on the Use of Cryptographic Controls |  |
| A.10.1.1 | Policy on the use of  cryptographic controls | YES | ISMS Enforcement | Control objectives | Policy on the Use of Cryptographic Controls |  |
| A.10.1.2 | Key management | YES | ISMS Enforcement | ISO/IEC 27001 | Policy on the Use of Cryptographic Controls |  |
| A.11 | Physical and environmental security | YES | ISMS Enforcement | Control objectives | Access Control Policy |  |
| A.11.1 | Secure areas | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy |  |
| A.11.1.1 | Physical security  perimeter | YES | ISMS Enforcement | Control objectives | Areas with sensitive information are protected describe how – walls, etc. |  |
| A.11.1.2 | Physical entry controls | YES | ISMS Enforcement | ISO/IEC 27001 | Access to the organization's secure areas must be controlled describe how – access cards, manned front entrance, etc. |  |
| A.11.1.3 | Securing offices,  rooms and facilities | YES | ISMS Enforcement | Control objectives | The facilities cannot be accessed from public areas, and secure areas are not noticeable to outsiders |  |
| A.11.1.4 | Protecting against  external and environmental  threats | YES | ISMS Enforcement | ISO/IEC 27001 | An alarm system is installed and linked to the alarm monitoring center of [name of security service provider]; surveillance cameras are installed; fire protection is implemented [describe how]; flood protection is implemented |  |
| A.11.1.5 | Working in secure  areas | YES | ISMS Enforcement | Control objectives | Procedures for working in secure areas |  |
| A.11.1.6 | Delivery and loading  areas | YES | ISMS Enforcement | ISO/IEC 27001 | Public access areas are controlled and delivery and loading areas in the ground are controlled |  |
| A.11.2 | Equipment | YES | ISMS Enforcement | Control objectives | Access Control Policy |  |
| A.11.2.1 | Equipment siting and protection | YES | ISMS Enforcement | ISO/IEC 27001 | All equipment is located in a physically protected area, and highly sensitive equipment specify which is located in Colocity |  |
| A.11.2.2 | Supporting utilities | YES | ISMS Enforcement | Control objectives | Devices for uninterruptible power supply [ for which IT and other equipment are installed] |  |
| A.11.2.3 | Cabling security | YES | ISMS Enforcement | ISO/IEC 27001 | Energy and data cables are installed within the secured area of the organization, and where this was not possible, they are protected [specify how] |  |
| A.11.2.4 | Equipment maintenance | YES | ISMS Enforcement | Control objectives | IT Dept. Head must keep a maintenance record for all equipment in accordance with the manufacturer's instructions, and ensure adequate maintenance in a timely manner |  |
| A.11.2.5 | Removal of assets | YES | ISMS Enforcement | ISO/IEC 27001 | Acceptable Use Policy |  |
| A.11.2.6 | Security of equipment  and assets off-premises | YES | ISMS Enforcement | Control objectives | [Acceptable Use Policy] / BYOD |  |
| A.11.2.7 | Secure disposal or reuse of equipment | YES | ISMS Enforcement | ISO/IEC 27001 | Operating Procedures for Information and Communication Technology / Disposal and Destruction Policy |  |
| A.11.2.8 | Unattended user  equipment | YES | ISMS Enforcement | Control objectives | Acceptable Use Policy / Clear Desk and Clear Screen Policy |  |
| A.11.2.9 | Clear desk and clear screen policy | YES | ISMS Enforcement | ISO/IEC 27001 | Acceptable Use Policy / Clear Desk and Clear Screen Policy |  |
| A.12 | Operations security | YES | ISMS Enforcement | Control objectives | Access Control Policy |  |
| A.12.1 | Operational procedures and responsibilities | YES | ISMS Enforcement | ISO/IEC 27001 | Access Control Policy |  |
| A.12.1.1 | Documented operating  procedures | YES | ISMS Enforcement | Control objectives | Operating Procedures for Information and Communication Technology |  |
| A.12.1.2 | Change management | YES | ISMS Enforcement | ISO/IEC 27001 | Operating Procedures for Information and Communication Technology / Change Management Policy |  |
| A.12.1.3 | Capacity management | YES | ISMS Enforcement | Control objectives | IT Dept. Head is responsible for monitoring the use of ICT assets and for planning required capacity |  |
| A.12.1.4 | Separation of development,  testing and  operational environments | YES | ISMS Enforcement | ISO/IEC 27001 | Development, testing and operational systems are separated |  |
| A.12.2 | Protection from malware | YES | ISMS Enforcement | Control objectives | Anti Viral & Malware Protection |  |
| A.12.2.1 | Controls against malware | YES | ISMS Enforcement | ISO/IEC 27001 | The tool in use is Windows Defender Security Center, Acceptable Use Policy |  |
| A.12.3 | Backup | YES | ISMS Enforcement | Control objectives | System Backup |  |
| A.12.3.1 | Information backup | YES | ISMS Enforcement | ISO/IEC 27001 | Operating Procedures for Information and Communication Technology / Backup Policy, Acceptable Use Policy |  |
| A.12.4 | Logging and monitoring | YES | ISMS Enforcement | Control objectives | System Logs |  |
| A.12.4.1 | Event logging | YES | ISMS Enforcement | ISO/IEC 27001 | System Logs |  |
| A.12.4.2 | Protection of log information | YES | ISMS Enforcement | Control objectives | Logs may not be deleted without permission granted by the authorized person e.g. IT Dept. Head |  |
| A.12.4.3 | Administrator and  operator logs | YES | ISMS Enforcement | ISO/IEC 27001 | System Logs |  |
| A.12.4.4 | Clock synchronization | YES | ISMS Enforcement | Control objectives | NTP System |  |
| A.12.5 | Control of operational software | YES | ISMS Enforcement | ISO/IEC 27001 | Acceptable Use Policy |  |
| A.12.5.1 | Installation of software  on operational  systems | YES | ISMS Enforcement | Control objectives | Acceptable Use Policy |  |
| A.12.6 | Technical vulnerability management | YES | ISMS Enforcement | ISO/IEC 27001 | HW & SW, Risk & Vulnerability |  |
| A.12.6.1 | Management of technical  vulnerabilities | YES | ISMS Enforcement | Control objectives | IT Dept. Head is responsible for monitoring all vulnerabilities of applications and other systems, and IT Dept. Head must select actions to be taken in case new vulnerabilities are identified |  |
| A.12.6.2 | Restrictions on software  installation | YES | ISMS Enforcement | ISO/IEC 27001 | Acceptable Use Policy |  |
| A.12.7 | Information systems audit considerations | YES | ISMS Enforcement | Control objectives | Audit/Risk Mgmt |  |
| A.12.7.1 | Information systems  audit controls | YES | ISMS Enforcement | ISO/IEC 27001 | Each audit is planned and coordinated with management; audits are performed only on read-only access rights |  |
| A.13 | Communications security | YES | ISMS Enforcement | Control objectives | Communication Matrix |  |
| A.13.1 | Network security management | YES | ISMS Enforcement | ISO/IEC 27001 | ACL through Firewall |  |
| A.13.1.1 | Network controls | YES | ISMS Enforcement | Control objectives | Operating Procedures for Information and Communication Technology/ Access Control |  |
| A.13.1.2 | Security of network  services | YES | ISMS Enforcement | ISO/IEC 27001 | Operating Procedures for Information and Communication Technology, Security Policy |  |
| A.13.1.3 | Segregation in networks | YES | ISMS Enforcement | Control objectives | The network is segregated in the following fashion:  The Back-end office network and the revenue generation network/retail network must be physically separated or segmented where all intranet resources must only be available to the company employees, not to the client |  |
| A.13.2 | Information transfer | YES | ISMS Enforcement | ISO/IEC 27001 | USB, Security |  |
| A.13.2.1 | Information transfer  policies and procedures | YES | ISMS Enforcement | Control objectives | Operating Procedures for Information and Communication Technology / Information Transfer Policy, Bring Your Own Device (BYOD) Policy |  |
| A.13.2.2 | Agreements on information  transfer | YES | ISMS Enforcement | ISO/IEC 27001 | [Operating Procedures for Information and Communication Technology / Information Transfer Policy |  |
| A.13.2.3 | Electronic messaging | YES | ISMS Enforcement | Control objectives | Information Classification Policy, Acceptable Use Policy |  |
| A.13.2.4 | Confidentiality or nondisclosure  agreements | YES | ISMS Enforcement | ISO/IEC 27001 | The form of Confidentiality Statement is pre-defined |  |
| A.14 | System acquisition, development and maintenance | YES | ISMS Enforcement | Control objectives | Pre-defined hardened environment |  |
| A.14.1 | Security requirements of information systems | YES | ISMS Enforcement | ISO/IEC 27001 | Pre-defined hardened environment |  |
| A.14.1.1 | Information security  requirements analysis  and specification | YES | ISMS Enforcement | Control objectives | When acquiring new information systems or changing existing ones, IT Dept. Head must document security requirements in the [Security Requirements Specification |  |
| A.14.1.2 | Securing application  services on public  networks | YES | ISMS Enforcement | ISO/IEC 27001 | Secure Development Policy |  |
| A.14.1.3 | Protecting application  services transactions | YES | ISMS Enforcement | Control objectives | Secure Development Policy |  |
| A.14.2 | Security in development and support processes | YES | ISMS Enforcement | ISO/IEC 27001 | Pre-defined hardened environment |  |
| A.14.2.1 | Secure development policy | YES | ISMS Enforcement | Control objectives | Secure Development Policy |  |
| A.14.2.2 | System change control  procedures | YES | ISMS Enforcement | ISO/IEC 27001 | Secure Development Policy |  |
| A.14.2.3 | Technical review of  applications after  operating platform  changes | YES | ISMS Enforcement | Control objectives | IT Dept. Head is responsible for reviewing and testing all applications after operating system changes, before they are put into production |  |
| A.14.2.4 | Restrictions on  changes to software  packages | YES | ISMS Enforcement | ISO/IEC 27001 | Operating Procedures for Information and Communication Technology / Change Management Policy |  |
| A.14.2.5 | Secure system engineering  principles | YES | ISMS Enforcement | Control objectives | Secure Development Policy |  |
| A.14.2.6 | Secure development  environment | YES | ISMS Enforcement | ISO/IEC 27001 | Secure Development Policy |  |
| A.14.2.7 | Outsourced development | YES | ISMS Enforcement | Control objectives | Supplier Security Policy, Secure Development Policy |  |
| A.14.2.8 | System security testing | YES | ISMS Enforcement | ISO/IEC 27001 | Secure Development Policy |  |
| A.14.2.9 | System acceptance  testing | YES | ISMS Enforcement | Control objectives | Secure Development Policy |  |
| A.14.3 | Test data | YES | ISMS Enforcement | ISO/IEC 27001 | QA |  |
| A.14.3.1 | Protection of test data | YES | ISMS Enforcement | Control objectives | Secure Development Policy |  |
| A.15 | Supplier relationships | YES | ISMS Enforcement | ISO/IEC 27001 | EXCLUSION |  |
| A.15.1 | Information security in supplier relationships | YES | ISMS Enforcement | Control objectives | EXCLUSION |  |
| A.15.1.1 | Information security  policy for supplier  relationships | YES | ISMS Enforcement | ISO/IEC 27001 | EXCLUSION |  |
| A.15.1.2 | Addressing security  within supplier agreements | YES | ISMS Enforcement | Control objectives | EXCLUSION |  |
| A.15.1.3 | Information and communication  technology  supply chain | YES | ISMS Enforcement | ISO/IEC 27001 | EXCLUSION |  |
| A.15.2 | Supplier service delivery management | YES | ISMS Enforcement | Control objectives | EXCLUSION |  |
| A.15.2.1 | Monitoring and review  of supplier services | YES | ISMS Enforcement | ISO/IEC 27001 | EXCLUSION |  |
| A.15.2.2 | Managing changes to  supplier services | YES | ISMS Enforcement | Control objectives | EXCLUSION |  |
| A.16 | Information security incident management | YES | ISMS Enforcement | ISO/IEC 27001 | Incident Mgmt. Policy & Process |  |
| A.16.1 | Management of information security incidents and improvements | YES | ISMS Enforcement | Control objectives | Incident Mgmt. Policy & Process |  |
| A.16.1.1 | Responsibilities and  procedures | YES | ISMS Enforcement | ISO/IEC 27001 | Incident Management Procedure |  |
| A.16.1.2 | Reporting information  security events | YES | ISMS Enforcement | Control objectives | Incident Management Procedure |  |
| A.16.1.3 | Reporting information  security weaknesses | YES | ISMS Enforcement | ISO/IEC 27001 | Incident Management Procedure |  |
| A.16.1.4 | Assessment of and  decision on information  security events | YES | ISMS Enforcement | Control objectives | Incident Management Procedure |  |
| A.16.1.5 | Response to information  security incidents | YES | ISMS Enforcement | ISO/IEC 27001 | Incident Management Procedure, Incident Response Plan |  |
| A.16.1.6 | Learning from  information security  incidents | YES | ISMS Enforcement | Control objectives | [Incident Management Procedure |  |
| A.16.1.7 | Collection of evidence | YES | ISMS Enforcement | ISO/IEC 27001 | Incident Management Procedure |  |
| A.17 | Information security aspects of business continuity management | YES | ISMS Enforcement | Control objectives | BCP Plan |  |
| A.17.1 | Information security continuity | YES | ISMS Enforcement | ISO/IEC 27001 |  |  |
| A.17.1.1 | Planning information  security continuity | YES | ISMS Enforcement | Control objectives | Procedure for Identification of Requirements, Business Continuity Policy, Business Impact Analysis Methodology, Business Continuity Strategy |  |
| A.17.1.2 | Implementing information  security continuity | YES | ISMS Enforcement | ISO/IEC 27001 | Business Continuity Plan |  |
| A.17.1.3 | Verify, review and  evaluate information  security continuity | YES | ISMS Enforcement | Control objectives | BCMS Maintenance and Review Plan, Exercising and Testing Plan, Post-incident Review Form |  |
| A.17.2 | Redundancies | YES | ISMS Enforcement | ISO/IEC 27001 | BCMS Maintenance and Review Plan |  |
| A.17.2.1 | Availability of information  processing  facilities | YES | ISMS Enforcement | Control objectives | Recovery strategy for IT infrastructure |  |
| A.18 | Compliance | YES | ISMS Enforcement | ISO/IEC 27001 | PCI-DSS, PA-DSS, ISO 27001, ISO 9001 etc. |  |
| A.18.1 | Compliance with legal and contractual requirements | YES | ISMS Enforcement | Control objectives | BCMS Maintenance and Review Plan |  |
| A.18.1.1 | Identification of applicable  legislation and  contractual requirements | YES | ISMS Enforcement | ISO/IEC 27001 | BCMS Maintenance and Review Plan |  |
| A.18.1.2 | Intellectual property  rights | YES | ISMS Enforcement | Control objectives | Acceptable Use Policy |  |
| A.18.1.3 | Protection of records | YES | ISMS Enforcement | ISO/IEC 27001 | Server Integrated |  |
| A.18.1.4 | Privacy and protection  of personally identifiable  information | YES | ISMS Enforcement | Control objectives | HoIT is responsible for implementing legal requirements related to personal data protection in the system |  |
| A.18.1.5 | Regulation of cryptographic  controls | YES | ISMS Enforcement | ISO/IEC 27001 | Encryption and Key Management Policy |  |
| A.18.2 | Information security reviews | YES | ISMS Enforcement | Control objectives | Information security policy review per year |  |
| A.18.2.1 | Independent review of  information security | YES | ISMS Enforcement | ISO/IEC 27001 | Internal Audit Procedure, certification audit by ASSIST |  |
| A.18.2.2 | Compliance with  security policies and  standards | YES | ISMS Enforcement | Control objectives | All owners of information assets, as well as the management, regularly review the implementation of security controls |  |
| A.18.2.3 | Technical compliance  review | YES | ISMS Enforcement | ISO/IEC 27001 | IT Dept. Head is responsible for checking the technical compliance of information systems with security requirements |  |

# Acceptance of Residual Risks

Since not all risks could be reduced in the risk management process, all residual risks are hereby accepted:

1. all risks with the value 0, 1 or 2
2. risks which could not be reduced to the abovementioned levels after the application of controls, according to the following table:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Name of asset** | **Asset owner** | **Threat** | **Vulnerability** | **New impact** | **New probability** | **Residual risk** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Validity and document management

This document is valid as of 27th March 2019

The owner of this document is IT Dept. Head who must check and, if necessary, update the document at least once a year, and immediately after risk assessment review and updates to the Risk Assessment Table and Risk Treatment Table.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

* number of nonconformities due to unclearly defined implementation method of individual controls
* number of nonconformities due to unclearly defined control objectives
* number of controls for which the achievement of objectives cannot be measured

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| **Owner** | **Title** | **Date** | **Signature** |
| Policy Author | Head of Technology | 1/11/2018 |  |
| **Approved By** | **Title** | **Date** | **Signature** |
| Executive Sponsor | Redwan-ul K. Ansari | 1/11/2018 |  |