SELCOM PAYTECH LIMITED

IT ACCESS AND USER MANAGEMENT POLICY

Contents

1 Policy Statement

Selcom will establish specific requirements for protecting information and information systemsagainst unauthorized access and will effectively communicate the need for information and information system access control.

2 Purpose

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important, asset for Selcom which must be managed with care. All information has a value to the company. However, not all this informationhas an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to usedifferent information resources and by guarding against unauthorized use.

Formal procedures must control how access to information is granted and how such access ischanged.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3 Scope

This policy applies to all Employees of Selcom (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Selcom with anyform of access to Selcom information and information systems.

4 Definition

Access control rules and procedures are required to regulate who can access Selcom information resources or systems and the associated access privileges. This policy applies always and should be adhered to whenever accessing Selcom information in any format, and on any device.

5 Risks

On occasion business information may be disclosed or accessed prematurely, accidentally orunlawfully. Individuals or companies, without the correct authorization and clearance may intentionally or accidentally gain unauthorized access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of theSelcom and may result in financial loss and an inability to provide necessary services to our customers.

6 Applying the Policy - Passwords

Choosing Passwords

Passwords are the first line of defense for our ICT systems and together with the user ID help toestablish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality,integrity or availability of our computers and systems.

Weak and *strong* passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with thehelp of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least eight characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).
- Same password cannot be used within 1 month's period
- Password should not contain your username
- Failed attempts 3 times will lead to account block till Administrator can unlock it

Example of Strong Password: pAsW17!^G

Protecting Passwords

It is of utmost importance that the password remains protected always. The following guidelinesmust be adhered to always.

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Selcom systems.
- Do not use the same password for systems inside and outside of work.

Changing Passwords

All user-level passwords must be changed at a maximum of every 90 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If youbecome aware, or suspect, that your password has become known to someone else, you **must**change it immediately and report your concern to your *supervisor* and *Technology and Software Development Department*

Users **must not** reuse the same password within 20 password changes

System Administration Standards

The password administration process for individual Selcom systems is well-managed andavailable to designated individuals only.

All IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.
- All Users which are in-active for 90 Days will be suspended for usage

7 Applying the Policy – Employee Access

User Access Management

Formal user access control procedures are documented, implemented and kept up to datefor each application and information system to ensure authorized user access and to prevent unauthorized access. They cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access or any staff who has left the company. Each user must be allocated accessrights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to usersthat are required to perform system administration tasks.

User/staff Registration

A request for access to the Selcom's computer systems must first be submitted to Individuals department for approval after which the form/access document will be sent to *Technology and Software Development* for further processing. Applications for access must only be submitted if approval has been gained from Head of Department and Compliance Unit.

When an employee leaves the Selcom, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibilityof the HOD to request the suspension of the access rights via the *Technology and Software Development.*

User Responsibilities

It is a user's responsibility to prevent their USER ID and password being used to gainunauthorized access to Selcom systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Inform relevant department for any changes to their role and access requirements.

Network Access Control

The use of modems on non-Selcom owned PC's connected to the Selcom's network can seriously compromise the security of the network. The normal operation of the network mustnot be interfered with. Specific approval must be obtained from HOD or *Technology and Software Development* before connecting any equipment to the Selcom's network.

User Authentication for External Connections

Where remote access to the Selcom network is required, an application must be made via the *Technology and Software Development*. Remote access to the network must be secured by two factor authentications consisting of a username and one other component, for example a Token based or SMS Based Token Number.

Supplier's Remote Access to the Selcom Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Selcom's network without permission from Technology and Software Development. Any changes to supplier's connections must be immediately sent to the Technology and Software Developmentor Compliance Unit, so that access can be updated or ceased. All permissions and access methods must be controlled by Technology and Software Development.

Partners or 3rd party suppliers must contact the Technology and Software Development before connecting to the Selcom network and a log of activity must be maintained. Remote access software must be disabled when not in use.

Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorized users are allowed.

All access to operating systems is via a unique login id that will be audited and can be tracedback to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged andaudited. The administrator account must not be used by individuals for normal day to dayactivities.

Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The Technology and Software Development along with software application users are responsible for granting access to the information within the system. The access must

- Be compliant with the User Access Management and the Password Procedure
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorized higher levels of access.
- Be logged and auditable.

User Access Review

- Generate Users from the System i.e. Active Directory and Application Systems
- Review their access level, if changes are required to be updated and documented
- Remove users who are no longer required or left the company
- Update User-List and access rights
- Monitor logs for their access are not over-lapping or incorrect access is not given
- Monitor inactive users in the system.
- Modify Users role for providing Administrative access will take up to 24 Hours as partof policy.

Privileged Account Management

- Selcom has selected only two (2) system admin for managing user accounts
- These accounts will be audited/reviewed on periodic basis or when required
- Access for privileged accounts can be revoked at any given time if threat or any activity found which is harmful to the company information security

8 Policy Compliance

If any user is found to have breached this policy, they may be subject to Selcom's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

The Policy of breaching is maintained by HR/Admin Department.

9 Policy Governance

The following table identifies who within Selcom is Accountable, Responsible, Informed orConsulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	CEO, Compliance Officer and Head of Technology and Software Department
Accountable	All HOD are accountable on their individual Staff access
Consulted	Compliance Unit and Technology and Software Department
Informed	All Staff Internal and External

10 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by IT Compliance Officer and Head of Technology and Software Department

11 References

The following Selcom policy documents are directly relevant to this policy, and are referencedwithin this document

- Remote Working Policy.

The following Selcom policy documents are indirectly relevant to this policy [amend list asappropriate]:

- Email Policy.
- Business Continuity Policy.
- IT Security Policy

12 Key Messages

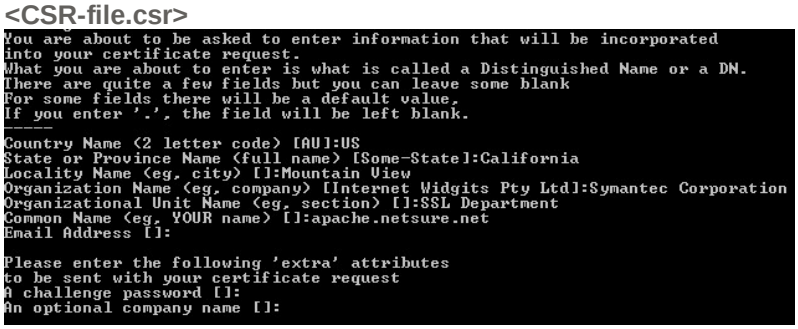
- All users must use **strong** passwords.
- Passwords must be protected always and must be changed at least every 90 days.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their USER ID and password being used to gain unauthorized access to Selcom systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Selcom's network without permission from Technology and Software Development
- Partners or 3rd party suppliers must contact the Technology and Software Development before connecting to the Selcom network.

13. PCI DSS Requirement on Key Management

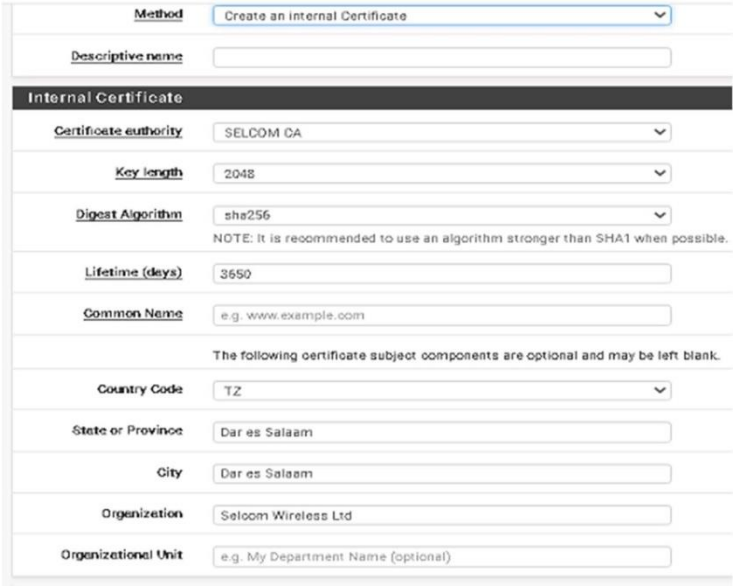
- Only Selected staff are required to generate keys to be send to Mastercard for Encrypting certificates provided for connectivity .
- Key documents are signed by 2 staff only.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their USER ID and password being used to gain unauthorized access to Selcom systems.
- Card Data should not be stored within Selcom Network, Database, or any medium or storage devices
- Key Management processed followed according to Mastercard Rules by PTS, for submitting individual forms for each staff who is authorized to generate the key and registered with Mastercard. Please refer to PKI Documentation of Mastercard
- Procedure for Generating Certificate (CSR)
    - 2 registered (with Mastercard) and authorized IT staff can generate CSR for Mastercard Key Exchange
    - Using OPENSSL or PFSENSE Firewall CSR generation tool

Command to use with OPENSSL:

openssl req -new -key <private-key-file.key> -config "Path" -out <CSR-file.csr>

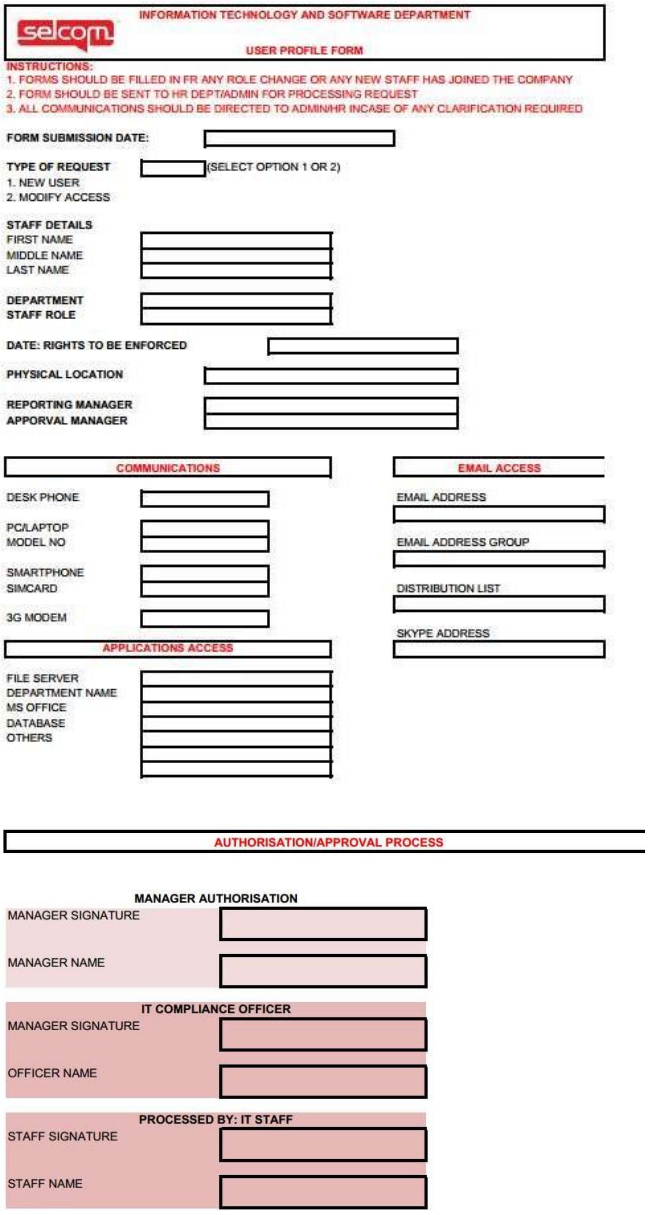


PFSENSE Tool:



13 Appendix 1

1. User Profile Form



INFORMATION TECHNOLOGY AND SOFTWARE DEPARTMENT

USER PROFILE FORM

INSTRUCTIONS:
1. FORMS SHOULD BE FILLED IN FR ANY ROLE CHANGE OR ANY NEW STAFF HAS JOINED THE COMPANY
2. FORM SHOULD BE SENT TO HR DEPT/ADMIN FOR PROCESSING REQUEST
3. ALL COMMUNICATIONS SHOULD BE DIRECTED TO ADMIN/HR INCASE OF ANY CLARIFICATION REQUIRED

FORM SUBMISSION DATE:

TYPE OF REQUEST (SELECT OPTION 1 OR 2)
1. NEW USER
2. MODIFY ACCESS

STAFF DETAILS
FIRST NAME
MIDDLE NAME
LAST NAME

DEPARTMENT
STAFF ROLE

DATE: RIGHTS TO BE ENFORCED

PHYSICAL LOCATION

REPORTING MANAGER
APPORVAL MANAGER

COMMUNICATIONS

DESK PHONE

PC/LAPTOP
MODEL NO

SMARTPHONE
SIMCARD

3G MODEM

EMAIL ACCESS

EMAIL ADDRESS

EMAIL ADDRESS GROUP

DISTRIBUTION LIST

SKYPE ADDRESS

APPLICATIONS ACCESS

FILE SERVER
DEPARTMENT NAME
MS OFFICE
DATABASE
OTHERS

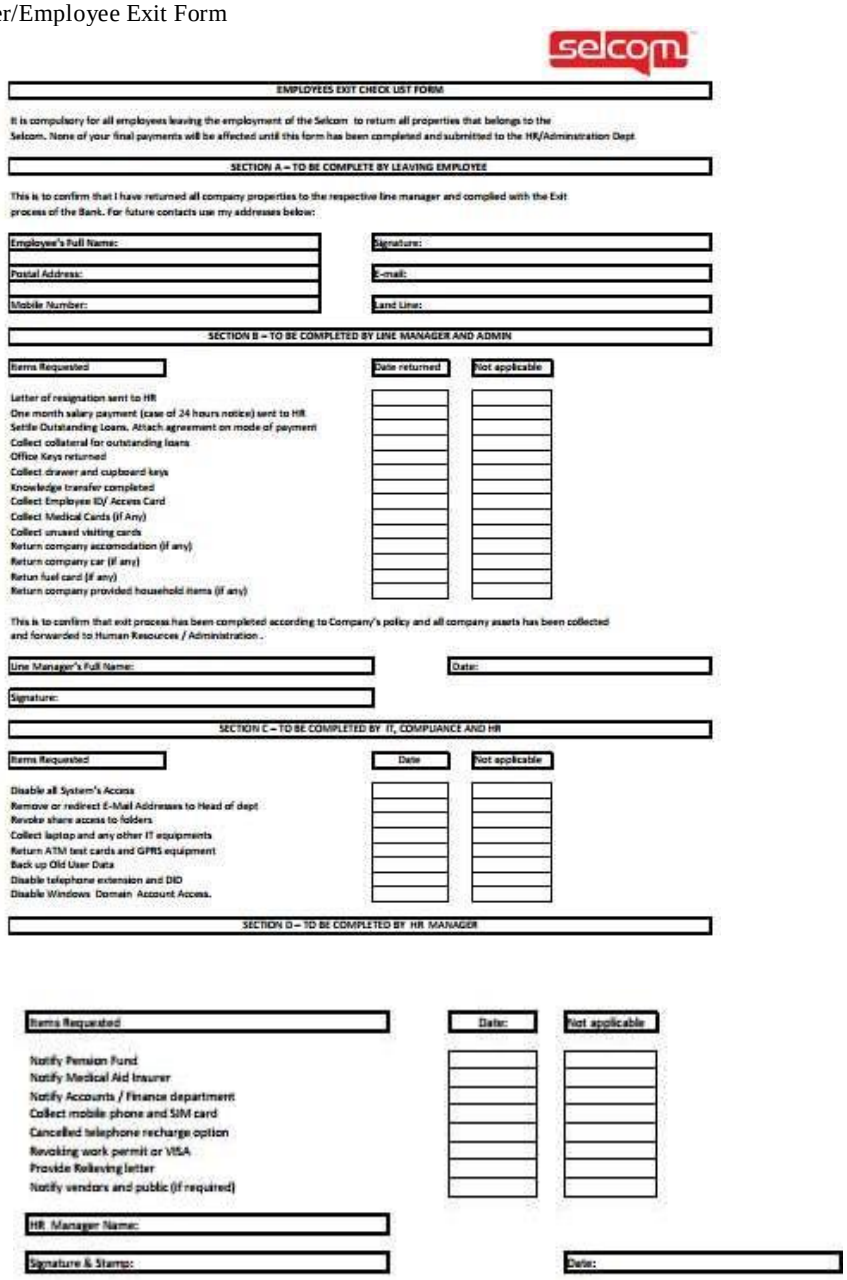
AUTHORISATION/APPROVAL PROCESS

MANAGER AUTHORISATION
MANAGER SIGNATURE
MANAGER NAME

IT COMPLIANCE OFFICER
MANAGER SIGNATURE
OFFICER NAME

PROCESSED BY: IT STAFF
STAFF SIGNATURE
STAFF NAME

2. User/Employee Exit Form



EMPLOYEES EXIT CHECK LIST FORM

It is compulsory for all employees leaving the employment of the Selcom to return all properties that belongs to the Selcom. None of your final payments will be affected until this form has been completed and submitted to the HR/Administration Dept

SECTION A – TO BE COMPLETE BY LEAVING EMPLOYEE

This is to confirm that I have returned all company properties to the respective line manager and complied with the Exit process of the Bank. For future contacts use my addresses below:

Employee's Full Name:	Signature:
Postal Address:	E-mail:
Mobile Number:	Land Line:

SECTION B – TO BE COMPLETED BY LINE MANAGER AND ADMIN

Items Requested	Date returned	Not applicable
Letter of resignation sent to HR		
One month salary payment (case of 24 hours notice) sent to HR		
Settle Outstanding Loans. Attach agreement on mode of payment		
Collect collateral for outstanding loans		
Office Keys returned		
Collect drawer and cupboard keys		
Knowledge transfer completed		
Collect Employee ID/ Access Card		
Collect Medical Cards (if Any)		
Collect unused visiting cards		
Return company accomodation (if any)		
Return company car (if any)		
Retun fuel card (if any)		
Return company provided household items (if any)		

This is to confirm that exit process has been completed according to Company's policy and all company assets has been collected and forwarded to Human Resources / Administration .

Line Manager's Full Name:	Date:
Signature:	

SECTION C – TO BE COMPLETED BY IT, COMPLIANCE AND HR

Items Requested	Date	Not applicable
Disable all System's Access		
Remove or redirect E-Mail Addresses to Head of dept		
Revoke share access to folders		
Collect laptop and any other IT equipments		
Return ATM test cards and GPRS equipment		
Back up Old User Data		
Disable telephone extension and DID		
Disable Windows Domain Account Access.		

SECTION D – TO BE COMPLETED BY HR MANAGER

Items Requested	Date:	Not applicable
Notify Pension Fund		
Notify Medical Aid Insurer		
Notify Accounts / Finance department		
Collect mobile phone and SIM card		
Cancelled telephone recharge option		
Revoking work permit or VISA		
Provide Relieving letter		
Notify vendors and public (if required)		

HR Manager Name:	
Signature & Stamp:	Date:

3. Declaration of Secrecy Form

DECLARATION OF SECRECY

This day _____of_____2017 I,_____the undersigned being the employee of Selcom (the company) do hereby undertake to keep secret on any information which shall come to me regarding the affairs of the company, all the communication facilitated under its service and comply with the right to privacy of the customers during my period of employment with the company excepting so far as I may be instructed in writing by Executive Director or his authorised representative(s) to divulge the same or except in so far as I may be called upon by the court of law to divulge the same.

I will deliver to the Company all working papers, computer tools and tapes or other material and copies provided to or prepared upon termination of the employment, for whatever reason.

_____
Employee's Signature

WITNESS':

Signature_____

Name _____

4. User Agreement

User Agreement

A user account with the IAR allows authorized personnel to access data from Selcom network that he/she can perform. This agreement outlines the responsibilities of the Staff. Possession of a user account entails responsibility to both your employer and employee and along with 3rd Party User

In return for being given a user account by your employer, you agree that:

1. You will comply with all relevant laws.
2. You will access and use only for the purposes of performing duties as mentioned in your job description. Furthermore, you will limit any access and use to what is necessary for these purposes.
3. You will maintain the confidentiality of all data at Selcom, and will not communicate this data to any other person.
4. If you become aware that the data has been compromised or leaked immediately report your Line Manager.
5. You will not disclose your password or secret code. You will not use any other person's password or secret code.
6. You will access the Selcom's Network and Database in accordance with these Terms and Conditions and any other conditions, policies and procedures that are required by your employer.
7. You understand that in agreeing to these Terms and Conditions, you are entering into a binding agreement with your employer.

In the event that you breach any of the provisions of this agreement, you may be subject to disciplinary actions up to (and including) dismissal. If these actions result in the suspension or revocation of your right to access PHI in the IAR as an Authorized User, the health care organizations participating in the IAR arrangement will be advised of the actions, as well as the rationale behind them.

_____
Name of Authorized User (Print):

_____ _____
Signature of Authorized User **Date**

Name of Authorized Supervisor (Print):

_____ _____
Signature of Supervisor **Date**

14 Document Control

Date	Version	Requester	Tech. Writer	Change/Review
21-06-2017	V1.0	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohamed
30--08-2017	V1.1	Deloitte/SCB	Mohammedjawaad Kassam. *Changes done to the document for Updating User Access Review policy 7.9* *Updating Document Control and Version details*	Sarah Mohammed
16--10-2017	V1.1	Deloitte/SCB	Mohammedjawaad Kassam. *Changes done to the document for Updating policy 7.10, 7.9 and 6.4* *Updating Document Control and Version details*	Sarah Mohammed
25--01-2020	V1.1	Kyte Consultants	Mohammedjawaad Kassam. *Changes to accommodate PCI Controls* *And include Key/CSR generation policy and procedure*	Sarah Mohammed