SELCOMPAYTECHLTD

Incident Management Policy

Contents

1. DocumentControl

Date	Version	Requester	Tech.Writer	Change/Review
21-06-2017	V1.0	SameerHirji	MohammedjawaadKassam	SarahMohamed
30--08-2017	V1.1	Deloitte/SCB	MohammedjawaadKassam *- Additionalcontentupdatefor informing SCB related issue. Section 7 of the document* *- DocumentControland Version Control Added*	SarahMohammed
29-09-2017	V1.1.	Kyte Consultants	AdditionalRequirementforPCI Zone	SarahMohammed
22-11-2018	V1.1.	Kyte Consultants	ReviewofPolicy	SarahMohammed
05-05-2018	V1.1.	Kyte Consultants	ReviewofPolicy	SarahMohammed
05-12-2019	V1.1.	Kyte Consultants	ReviewofPolicy	SarahMohammed

2. PolicyStatement

It is the policy of Selcom that any incident related to IT or Non- IT Related will be handled properly, effectivelyandinamanner,thatminimisestheadverseimpacttothecompanydailyoperation sandthe risk of data loss.

Selcomneedstoensurefollowing:-

- Incidentsarereportedinatimelymannerandcanbeproperlyinvestigated.
- IncidentsarehandledbyappropriatelyauthorizedandskilledpersonnelsuchHODorSupervis or
- Appropriatelevelsofmanagementareinvolvedinthedeterminationofresponseactions
- Incidentsarerecordedanddocumentedasperpolicy
- Theimpactoftheincidentsisunderstood,andactionistakentopreventfurtherdamage
- Evidenceisgathered,recordedandmaintainedinaformthatwillwithstandinternal andexternal scrutiny
- Externalbodiesordatasubjectsareinformedasrequired
- Theincidentsaredealtwithinatimelymannerandnormaloperationsrestored
- Theincidentsarereviewedtoidentifyimprovementsinpoliciesandprocedures.

Stafftrainingonincidentmanagementishandledinternallyby ITComplianceandTec hnologyand Software Development Team.

TheComplianceunitalongwithTechnologyandSoftwaredepartmentwillalsomonit orandreview information security incidents to identify recurring incidents and areas of risk. The review process willbeused to identifyrequirementsfornew orchangedpolicies,to updatetheriskregisterandto identify any other relevant controls.

AspartofdatasecuritySelcomwillcommunicatetoallstaffrelatedtoincidentManage mentalong with other policies to maintain data prevention and loss of Data.

3. **Scope**

ThispolicyappliestoallDepartments,Partners,EmployeesofSelcom,ICTfacilitiesandequipment,or have access to, or custody of, customer information.

Allusersmustunderstandandadoptuseofthispolicyandareresponsibleforensuringthesafetyand security of the Selcom information assets. All users have a role to play and a contribution to make to identifying potential risks to the safe and secure use of information and any Information technology.

4. **Definition**

The definition of an 'Information Incident' is an adverse event affecting an information asset that has caused or has the potential to have an adverse effect on the business operation or function, or Selcom,its service users, its employees, or its partners. Examples are physical harm, embarrassment or distress to individuals, damage to organizational reputation, financial impact etc. Incident management is concernedwithintrusion,theft,thecompromiseandmisuseofinformationandinformationresources,and the continuity of critical information processes. *Examples of Information Incidents are given in theAppendix*

5. **Policy**

Thispolicysetsoutheprinciplesforthemanagementofinformationincidentsbelow.

Theprinciplesare:

- Asingleinformationincidentcontactpointforalltypesofinformationincident (manual, electronic, etc.).
- Informationcapture/loggingofallinformationeventsconfirmedasincidents.
- Guidanceavailableforinformationusersonreportinginformationeventsandincidents.
- Progress/trackinginformationloggedfrominitialcontactthroughtoincidentresolution.
- Identifiedtimecriticaltaskswithsettargetsandescalationsteps.
- Assessmentofpotentialseverityasearlyaspossible,todeterminetheappropriateincident management actions.
- Standardassessmentofincidentseverityconsistentwithriskmanagementguidance.
- Highseverityorpotentialhighseverityincidentsortobereferredtothecomplianceunitassoon as identified.
- ProcedurestoallocateaninvestigationtoICTComplianceofficer.
- Specificprocedurestocoverincidentissuessuchascommunicationsprotocolsandpreservation and collection of evidence.
- SevereincidentswillbereportedinariskregisterandpresentedittotheSelcomManagement Board
- SummaryreportsofnonsevereincidentstoHeadofDepartments

- TheInformationRiskRegistertoincludeallidentifiedrisksarisingfrominformationincidents.

- Allproceduresmaintainedandreviewedannuallyorasrequired.Thoughallinforma tionincidents will be reported to a single contact point, distinction is drawn from that point between ICT technical incidents (e.g. malware, software malfunction, hacking incidents) and those involving disclosure of manual records or end user behavior, which will necessarily follow different investigation and incident management routes but should still comply with the above principles.

6. Responsibilities

- It is the responsibility of all Selcom information users to be able to identify potential security eventsandweaknessesandtotakeimmediateactiontoreportthesedirectlytothelin emanager or IT Compliance Officer

- AllLineManagersshouldensurethattheirstaffareawareoftheirobligationsunde rthispolicy and support them in meeting these obligations.

- Service Providers and Partnership Working Any information security incident that involves SELCOM information must be reported without delay. This should be a contractual requirement whereaservicecontractexistsandincludedinanyinformationsharingagreementfo rthesharing ofpersonalinformation. SELCOMmanagersandemployeesmustbeawareofsimilarobligations to other agencies if a security breach involves their information.

- Thecontactpointproceduresmustensurethatalleventsthatarereportedarepromp tlyrecorded and forwarded to the appropriate staff for action.

- HOofSoftwareDevelopmentandComplianceOfficerareresponsiblefordoc umentingand implementing the Selcom Incident management procedures.

- ITComplianceOfficerisresponsibleforensuringthatappropriateincidentmanage mentplansare put in place as soon as possible to deal with high impact incidents, is also responsible, with supportfromInformationOwners(users)for ensuringthat allincidentsaresubjecttoinvestigation and subject to information risk management processes.

- Audit Services are responsible for reviewing incident procedures and plans, providing advice wheresecuringevidenceisanissueandortheinvolvementofthePoliceispossible,u ndertaking investigations, undertaking reviews and providing advice.

7. **EscalationMatrix**

According to ITIL standards, although assignment may change, ownership of incidents always resideswiththeHelpdeskorOperationalstaff.Asaresult,theresponsibilityofensuringthatan incident is escalated when appropriate also resides with the Service Desk or Operational staff.

Within24HoursofIncident,Bankwillbenotifiedforthesameusingincidentmanagement document refer to Appendix

ComplianceUnitwillmonitorallincidents,andescalatethembasedonthefollowingguidelines:

Priority	TimeLimitbeforeEscalation	
3- Low	3businessdays	OperationalStaff/ Bank Officer
2- Medium	4hours	LineManager/ Bank Officer
	Ifon-callcontactcannotbereachedduringnon-businesshours	LineManager/ Bank Officer
	Ifneitheron-callcontactortheirLineManagercannotbereachedduring non-business hours	HOD/Bank Officer
	48 hours	HOD/Bank Officer
1- High	Immediate	LineManager/ Bank Officer
	Immediate	HOD/Bank Officer

FunctionalEscalation

When theCompliance Unit receives notification of an incident, they are toperform the initialidentificationanddiagnosistoclassifytheincidentaccordingtoservicecategory and prioritization.If the incident is a known problem with a known solution, the Unitwill attempt a resolution.If it is not a known problem or if the attempted solution fails,theywilldelegateresponsibilityforanincidenttoanappropriatechannel

EscalationNotifications:

Anytimeacaseisescalated,notificationwilloccurtovariousindividualsdependingupon the priority of the incident.Following are basic guidelines for notifications:

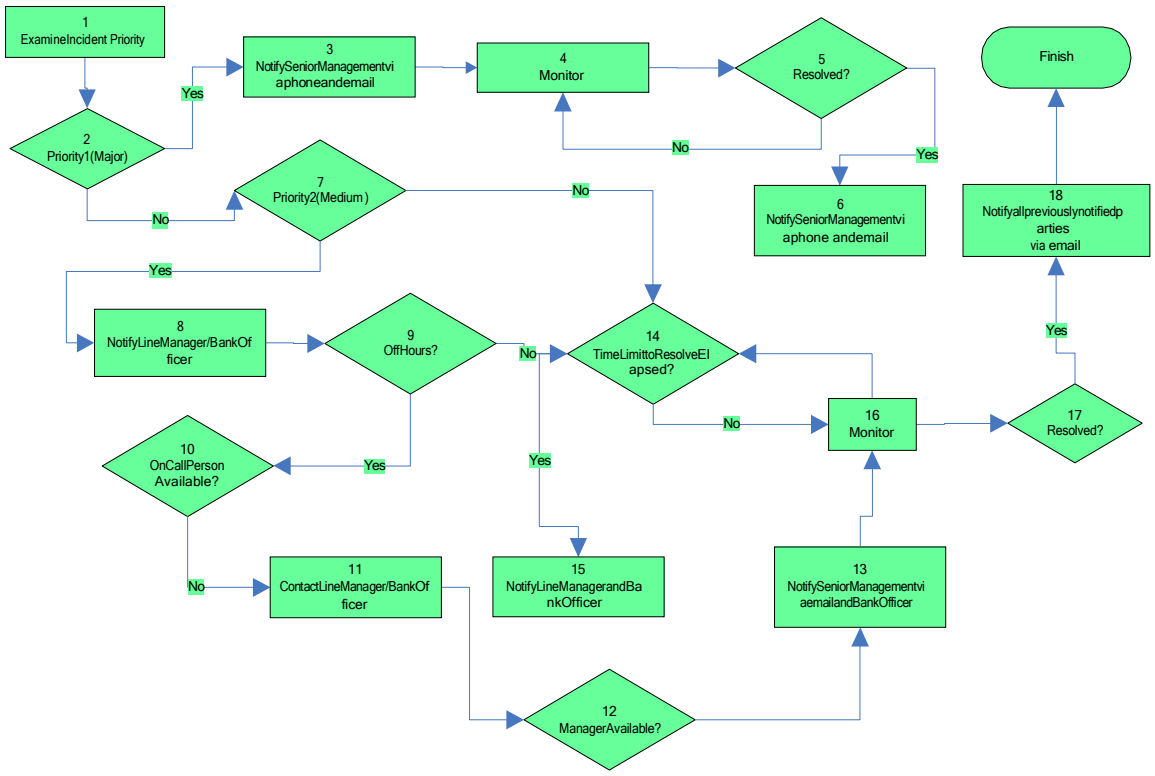
The default mechanism for notification will be by email unless otherwise specifically stated.Wheneverescalationornotificationbyphoneisindicated,allknownnumbers for contact should be utilized.Senior management notification will include HOD, Compliance Unit, and all functional Line Managers.Escalation of a case does not remove the assignment from an individual.It is up to the Line Manager to make certain that right personnel are assigned.When additional personnel need to be involved, they may be added as interested parties.

Anytimeacaseisescalated,thecasewillbeupdatedtoreflecttheescalationandthe following notifications will be performed. Person to whom

case is currently assigned will be notified.

BankSecurityorOperationaldepartmentwillbenotifiedforeveryincidentoccurred which is related to the service provisioned for Bank Specific

EscalationProcessDiagram



IncidentEscalationProcessSteps:

Allescalationprocessstepsareperformedbythecomplianceunit.Someoft hesteps may be automated.

Step	Description
➢	Examineallopenincidentsanddetermineactionsbaseduponincident priority.
➢	Isthisapriority1(highpriority)incident?
➢	Ifitisahighpriorityincident,immediatelynotifyLineandHODpersonnel. HOD personnel should be contacted by phone.
➢	Monitorthestatusofthepriority1incidentprovidinginformationalupdates to management at a minimum of every 1 hours.
➢	Hastheincidentbeenresolved?Ifnotcontinueto monitor.
➢	Iftheincidenthasbeenresolved,notifyLineManagerandHODofthe resolution.HOD should be notified by phone during business hours.
➢	Isthisapriority2(mediumpriority)incident?
➢	Ifso,notifytheLineManagerperformingtheresolution.Notificationshould be by email.
➢	Hastheincidentoccurredduringbusinesshoursoroffhours?Ifduring business hours, proceed to step 14.
➢	Iftheincidentoccurredduringoffhours,istheon-callpersonavailable?
➢	Iftheon-callpersonisnotavailable,calltheLineManagerofthe department assigned for resolution.
➢	▪ IstheLineManagerofthedepartmentavailable?
➢	Ifneitherthedepartmenton-callpersonortheLineManagerofthe department is available, notify HOD via email and phone.
➢	Hasthetimelimittoresolvetheincidentelapsed?
➢	Ifthetimelimittoresolvehaselapsed,notifytheLineManagerofthe department via email.
➢	Continuetomonitortheincident
➢	▪ Hastheincidentbeenresolved?
➢	▪ Iftheincidenthasbeenresolvednotifythecustomerandallpersonnel previously contacted of the resolution.

8. **PolicyGovernance**

ThefollowingtableidentifieswhowithinSelcomisAccountable,Responsible,Informed orConsulted with regards to this policy. The following definitions apply:

- Responsible-theperson(s)responsiblefordevelopingandimplementingthepolicy.
- Accountable-thepersonwhohasultimateaccountabilityandauthorityforthepolicy.
- Consulted-theperson(s)orgroupstobeconsultedpriortofinalpolicyimplementationor amendment.
- Informed-theperson(s)orgroupstobeinformedafterpolicyimplementationoramendment.

Responsible	CEO,ComplianceOfficerandHeadofTechnologyandSoftware Department
Accountable	AllHODareaccountableontheirindividualStaffaccess
Consulted	InternalComplianceandTechnologyandSoftwareDepartment
Informed	AllStaffInternalandExternal

9. **ReviewandRevision**

Thispolicywillbereviewedasitisdeemedappropriate,butnolessfrequentlythanevery12months. Policy review will be undertaken by Compliance Officer and Head of Technology and Software Department.

10. **PCIRequirement**

Thepolicyisrequiredtomonitorthelogsandmanageincidentbasedonthecategoryorcriteria,the Incident is considered following systems can generate an incident based on the severity of the log generated. The system are as follows but not limited to

- PhysicalAccessControl
- LogicalAccessControl
- Firewalls
- Anti-VirusSystems
- ActiveDirectoryManagements
- Auditloggingmechanisms

IncidentManagementandReportingwithinPCIZone

- Restoringsecurityfunctions
- Identifyinganddocumentingtheduration(dateandtimestarttoend)ofthe security failure
- Identifying and documenting cause(s) of failure,including root cause, and documenting remediation required to address root cause
- Identifyingandaddressinganysecurityissuesthatarоseduringthefailure
- Performingariskassessmenttodeterminewhetherfurtheractionsarerequired because of the security failure
- Implementingcontrols topreventcauseoffailure fromreoccurring
- Resumingmonitoringofsecuritycontrols

11. Appendix–

ExamplesofInformationSecurityEventsandIncidents

ExamplesofthemostcommonInformationSecurityEventsandIncidentsare listed below. It should be noted that this list is not exhaustive.

- Criminalevents:
  - Theftofequipment,dataorinformation,fraudorfraudulentactivities;
  - 'Bagging'offenceswhereinformationisobtainedbydeceptione.g.unknownpeople askingforinformation,suchasapasswordordetailsofathirdparty,thatcouldgain them access toCouncildata or receiving unsolicited mail that requires you toenter password data;
  - Attempts(eitherfailedorsuccessful)togainunauthorizedaccesstodataor information stored on computer systems e.g. hacking; Copyright issues;

- Technicalevents:
  - Changes to information or data or system hardware, firmware, or software characteristicswithouttheCouncil'sknowledge,instruction,orconsente.g.malware (viruses, Trojans etc.); use of unapproved or unlicensed software on Council equipment;
  - Unwanteddisruptionordenialofservicetoasysteme.g.spamattacks;receiving unsolicited mail of an offensive nature; receiving and forwarding chain letters including virus warnings, scam warnings and other emails that encourage the recipient to forward onto others;
  - Hardware/softwarefailures;

- PeopleEvents:
  - Accidentallossofequipment,dataorinformationincludinghandhelddevicessuchas Blackberries;
  - FailingtolockaPCscreenwhenleftunattended.
  - Human error e.g. emailing personal and/or sensitive personal information outside of theCouncil'snetworkeitherinerrororwithoutappropriatesecuritymeasuresinplace
  - Sharing/transferofdataorinformation,includingpersonaland/or
  - sensitive information with those who are not entitled to receive that information; withouttheconsentofthedatasubject;andsharingmorethantheneces saryamount of personal/sensitive information to complete required tasks.
  - Theunauthorizeduseofasystemfortheprocessingorstorageofdataby any person
  - Accessingcomputersystems/applicationsusingsomeoneelse's
  - authorizatione.g.useridandpassword;sharingaccesstokensorlogins;leaving your desk without logging off
  - Disclosureofpasswords/writingitdown,andleavingitondisplaywhereitwouldbe easy to find and used by unauthorized users;
  - Printingorcopyingconfidentialinformationandnotstoringitcorrectlyorconfidentially e.g.leavingdocumentsonphotocopiers.

- PhysicalandEnvironmentalevents:
  - Unforeseencircumstancese.g.fireorflood
  - Unsecurepremises
  - Unlocked/unsecuredworkstations

Risk Register for Incident Policy Management

RISK REGISTER FOR INCIDENT POLICY MANAGEMENT

RISK NO.	RISK DESCRIPTION (Event, Causes, Impacts)	RELATED OBJECTIVES (e.g. business, strategic, project)	DATE RISK ADDED (MM/DD/YYYY)	DATE RISK AND CONTROLS LAST ASSESSED (MM/DD/YYYY)	CONTROLS (What is in place to prevent, detect and manage risk?)	CONTROL EFFECTIVENESS RATING (high, medium, low)	LIKELIHOOD OF RISK SCORE (1-5)	CONSEQUENCE OF RISK SCORE (1-5)	RESIDUAL RISK RATING (Very high, high, medium, low)	CHANGE IN RISK RATING (Improving, No Change, Getting Worse)	RISK OWNER (Job Title)	RISK TREATMENT/S (accept, avoid, reduce, share risk source, change likelihood, change consequence)	STATUS OF TREATMENT PLAN (not commenced, in progress, completed)

Incident Management Document

Obligation	RoleDescription
Responsible	Responsibletoperformtheassignedtask
Accountable(only 1 person)	Accountabletomakecertainworkisassignedandperformed
Consulted	Consultedabouthowtoperformthetaskappropriately
Informed	Informedaboutkeyeventsregardingthetask

SNO	Activity	Personnel Assigned	Line Manager	HOD	Compliance	Resolution