Initial Incident Escalation Process Guide

Version:	2.0
Release Date:	May 2018
Status:	Final
Reviewed:	Information Services Risk and Compliance
Policy Owner:	Executive Manager Risk
Frequency of Review:	Annually

Contents

1. Scope

This management policy has been developed to outline the process for escalating critical issues to relevant managers to assess a situation and act accordingly. This should be at the first sign of any incident impacting members and Qudos Bank, and well before any incident is deemed to be a material issue under QB's Business Continuity Plan.

2. Version Control

Date	Reviewed By	Purpose/Change
May 2018	Cameron	Introduction of policy

3. Policy

3.1 Detection & Reporting

When an incident is identified or detected the staff member should immediately contact IT Support and inform their Manager. IT Support will analyse the incident and classify the severity based on the impact as outlined in the Severity classification table 3.2.

Upon classification of a severity 1 or 2 incident IT Support will contact the Executive Management incident response team and notify them of the incident.

The Executive Management incident team include:

Contact/Name	**Work Phone#**	**Title/Description**
David Bridges	0404 480 013	Executive Manager Technology
Stephen Swannell	0416 082 699	Executive Manager Retail Banking
Joff Stevens	0402 835 747	Executive Manager Strategic Marketing
Antar Chahine	0409 824 305	Executive Manager Risk and Compliance

3.2 Classification and Initial Support

Classification is the process of categorising and prioritising a given incident. Incidents must be classified so that the subsequent actions to be taken can be effectively determined.

Below outlines the definition of a severity 1- 4 issue and how to classify the severity along with the expected response to be taken when the incident is detected.

Severity	Business Impact	Description	Action Required	SMS Exec Team
1	Critical	Directly reducing ability to conduct business or significant impact to members ▪ Loss of Internet banking ▪ Loss of access to card switch (e.g. ATM, EFTPOS, VISA) ▪ Loss of access to payment gateway (e.g. Indue, Direct Entry, payroll) ▪ Loss of Core Banking ▪ More than 50% of staff members affected ▪ 2 or more Branches fails and cannot conduct normal business operations ▪ Contact Centre fails and cannot conduct business ▪ Issue causing direct compliance (e.g. settlement cut-off periods) or regulatory impact to QUDOS	▪ Alert IT Support ▪ IT Support to record incident and perform initial support ▪ IT Support to send out email notifications to staff ▪ IT Support to immediately send SMS Notification to the Executive Team ▪ IT Support to send regular updates and notifications to Executive team - every 30 minutes or when new information becomes available. ▪ Executive Management incident team to convene conference meeting to discuss and determine appropriate actions	✓ and a call immediately to Executive Team
2	Significant	Directly causing partial loss of ability to conduct business ▪ 1 channel is unavailable (IB, MB, Internet) ▪ Large number of Visa, EFTPOS or ATM services affected ▪ Large number of staff affected ▪ 1 Branch fails and cannot conduct normal business operations	▪ Alert IT Support ▪ IT Support to record incident and perform initial support ▪ IT Support to send out email notifications to staff ▪ IT Support to send SMS Notification to the Executive Team ▪ IT Support to send regular updates and notifications to Executive team - every 30 minutes or when new information becomes available. ▪ Executive Management incident team to convene conference meeting to	✓

			discuss and determine appropriate actions	
3	Standard	Directly reducing the productivity of some staff ▪ Core Banking or other application cannot be accessed by a single branch. ▪ Minimal client reach with localised problems and within control.	▪ IT Support to send out email notifications to staff ▪ IT Support to send regular updates when new information becomes available.	✖
4	Minor	▪ Causing only inconvenience and no impact or impairment of service and no immediate action required ○ <20% of business processes / system failure, redundancy activated ○ Scheduled activities are not affected	▪	n/a

3.3 Roles & Responsibilities

All staff have a responsibility to inform IT Support of any incident.

Information Services will have responsibility for managing the incident including recording and monitoring, investigating root cause and liaising with Executive Management team on any Severity 1 or 2 incidents.

Executive Management incident team will have responsibility for reviewing the incident in line with our BCP policy to determine the extent of the incident invoking a BCP incident. The Exec team will be responsibility for determining the required communications to publish to customers and staff, above and beyond the incident notifications from IT Support.