Managed Network Services – Change Management Framework

This document was last modified [November 2, 2021] and may updated from time to time by Datavalet.

1 CHANGE MANAGEMENT OVERVIEW

The Datavalet Change Management process is designed to control the life cycle of strategic, tactical, and operational changes to the managed IT services through standardized procedures.

A Change Request shall include the following:

- the reason for the proposed Change with estimated impact
- the procedure and time frame in which such Change is proposed to be made
- the estimated costs associated to the Change Request and the proposed allocation of said costs

Based on the service request received from the client, or for the necessary maintenance of the network, the following activities will be performed by Datavalet:

- Defining the change parameters
- Selecting the appropriate team members to perform the change
- Identify change accountability and related impact as well as securing required approval
- Develop the necessary implementation plan
- Implementing the change as planned
- Collect and analyze data on the result and potential impact of the change
- Complete the change with resulting status

2 CHANGE TYPES

The following types of changes will be leveraged and applied within the service

2.1 **Standard Changes:** A standard change is one that occurs frequently, is low risk and has a pre-established procedure with documented tasks for completion. Standard changes are subject to pre-approval to speed up the change management process.

2.2 **Normal Changes:** A normal change is one that is not standard and not emergency and typically requires an important change to a service or the managed IT infrastructure (which can encompass physical hardware changes or global configuration updates). A normal change is subject to the full change management review process, including review by the Change Advisory Board (CAB) and authorization/rejection.

2.3 **Major Changes:** A normal or emergency change that may have significant implications and/or be high risk. Such a change requires an in-depth change proposal with justification and appropriate levels of management approval.

2.4 **Emergency Changes:** An emergency change is one that must be assessed and implemented as quickly as possible to resolve or prevent a major incident. Emergency change need to be

approved by the client and Datavalet management (through emergency CAB procedure) to be performed but could be documented "after-the-fact".

Change Type	Request Type	Lead Time	Hour of execution
Standard	Type 1	2 Business days	Normal business hours 09:00 to 21:00EDT
Normal	Type 2	Evaluation - 2 Business days Execution – 3 Business days	Normal business hours 09:00 to 21:00EDT
Normal **(Global Configuration)**	Type 2	Evaluation - 5 Business days Execution – TBD	Extended business hours 06:00 to 24:00EDT
Normal **(Physical Change)**	Type 2	Evaluation - 2 Business days Execution – 15 Business days	Extended business hours 06:00 to 24:00EDT
Major	Type 3	Evaluation - 10 Business days Execution – TBD	TBD – per case basis

3 CHANGE MANAGEMENT SERVICE LEVELS

The categorizations and service levels for change management related activities are defined below.

Process	Measurement	SLO/SLA	Target
Request for Change (RFC) acknowledgement and response	$\left(\frac{RFC_{Submitted} - RFC_{LateResponse}}{RFC_{Submitted}}\right) * 100$	≥ 98% Within 8 business hours	100%
Successful Change implementation	$\left(\frac{RFC - RFC_{Incident}}{RFC}\right) * 100$	≥ 98% of Changes without Incident and within Allocated Time	100%

Process	Measurement	SLO/SLA	Target
Acknowledgement of Critical CVE	Assessing time of publication of critical CVE with written communication sent to customer	Notification of security concern within 8 hours	8 hours
Deployment of critical security hotfixes	((Total amount of in-scope devices – devices confirmed with the latest hotfix) divided by the Total amount of in-scope devices) x 100	80% of affected devices	24 hours

4 CHANGE CATALOG

Catalog #	Service Request	Type #	Service Delivery Duration
1	Access Control List change	1	2 days
2	Create/Remove/Modify Firewall (FW) rules/objects	1	2 days
3	Create/Edit Port-Channel	1	2 days
4	Existing DNS record modification	1	2 days
5	Create DNS record	2	5 days
6	Interface reset (shutdown/bring up)	1	2 days
7	Add IP SLO monitoring	1	2 days
8	Add/Remove device license	1	2 days
9	Update switch/access point IP	1	2 days
10	LDAP configuration for authentication	2	5 days
11	Add/Remove/Change NAT	1	2 days
12	Add/Remove/Change SSID	1	2 days
13	Port descriptions change	1	2 days
14	VLAN Change (trunk/access port)	2	5 days
15	Add/Remove/Change VPN Site to Site Configuration	2	5 days
16	Whitelist/Blacklist URL/IP at FW	1	2 days
17	Whitelist/Blacklist end user devices (portal bypass)	1	2 days
18	WAN Site/Hardware decommission	3	15 days
19	Access Point Name Change	1	2 days
20	Replace failed Access Point	1	2 days
21	Add/Remove/Change device to security module	1	2 days
22	Add/Remove/Change device to backup scripting	1	2 days
23	Add/Remove/Change TACACS/Radius setting to device	1	2 days
24	Add New Interface	2	5 days
25	Add/Remove/Change Port Forwarding	1	2 days
26	Create/Modify/Delete User Profile	1	2 days
27	Create/Modify/Delete Client Profile	2	5 days
28	Add/Remove/Change bandwidth limitation rules (quota)	3	15 days
29	Add/Remove/Change QoS policies	3	15 days
30	Configure Firewall logs forwarding	3	15 days

31	Add/Remove/Change BGP/MPLS VPN Interconnection	3	15 days
32	WPA Key change	1	2 days
33	Signal change (broadcast strength and channel)	1	2 days
34	DHCP scope change	1	2 days
35	Contact/escalation pat modification	1	2 days
36	Landing page modification	1	2 days
37	Deploying additional hardware*	3	15 days
38	Ad-hoc report customization	2	5 days
39	Business process modification	2	5 days
40	Modification of external authentication server type	2	5 days
41	On-site activity specifically requested by a designated customer contact*	3	15 days