

D2C2 NOC SOP

CONFIDENTIAL – FOR INTERNAL USE ONLY

Document Version: 4.7

Document Last Revision: 4/15/2021

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** | **Approver** |
| .1 | 3/18/221 | Jorge Neyra | Creation |  |
| .2 | 3/24/21 | Jorge Neyra | * Added an SDD section * Added CMDB * Added RCA procedure for P1 and P2 * Added escalation chart for P1, P2, and P3 incidents. |  |
| .3 | 3/26/21 | Jorge Neyra | * Added Backup section * Added Monitoring section * Added Business Continuity section * Added Patching section * Removed Incident Response * Removed Types of Incidents |  |
| .4 | 3/31/21 | Jorge Neyra | * Flowcharts updated * Updated CCB procedures * Added PW policy * VDI monitoring was added |  |
| 4.1 | 4/7/21 | Jorge Neyra | * Updated Create Account * Created Admin Access flow * Updated Change control to include Configuration * Included outages in the Incident Response flow |  |
| 4.2 | 4/8/21 | Jorge Neyra | * Added Backup validation steps * Added Snapshot procedure * Added daily backup checks for servers and databases * Added Restore steps |  |
| 4.3 | 4/9/21 | Jorge Neyra | * Removed Automate Health Check * Removed Automated Login Alerts * Removed System Monitoring * Removed VDI Monitoring |  |
| 4.4 | 4/10/21 | Jorge Neyra | * Added a procedure table * Removed Testing * Removed Training |  |
| 4.5 | 4/12/21 | Jorge Neyra | * Added User Login Security Rules under User Access * Updated Post Implementation process to include audits and reviews * Included a section on Logical Access Restrictions under Configuration Management section. |  |
| 4.6 | 4/13/21 | Jorge Neyra | * Included procedures for installing Monitoring and Logging agents under the Monitoring section * Updated User Termination policy to include system access disabled within 8 hours of employment termination * Added Password Recovery Procedures for GCP users * Added a Quarterly Task – review authorized software list by CAB * Added Software Access List as an Appendix |  |
| 4.7 | 4/15/21 | Jorge Neyra | * Added a Maintenance section. Rolled up Daily tasks to this section * Added a sub section under Maintenance titled Maintenance Test and Diagnostic Tools * Created a new procedure called Hourly Health Check |  |
| 4.9 | 4/21/21 | Jorge Neyra | * Updated the Incident Response P1 procedure * Included a Project column to the Server List appendix * Added a section on Vendor O&M * Added a procedure for Vendor Incidents |  |
| 4.12 | 5/17/21 | Jorge Neyra | * Updated the Updates and Patches procedure to include 1st stage approval by the Change Management team. |  |

Contents

[1.0 Introduction 9](#_Toc73446161)

[1.1 D2C2 Program 9](#_Toc73446162)

[1.2 Purpose 9](#_Toc73446163)

[2.0 Stakeholders 10](#_Toc73446164)

[3.0 Roles and Responsibilities 10](#_Toc73446165)

[3.1 Chief Information Security Officer (CISO) 10](#_Toc73446167)

[3.2 Project Chief Engineer 10](#_Toc73446168)

[3.5 Product SME 11](#_Toc73446169)

[3.6 System Administrator (SA) 11](#_Toc73446170)

[3.7 End-User 11](#_Toc73446171)

[4.0 Monitoring 12](#_Toc73446172)

[4.1 Incident Error Log Reviews 12](#_Toc73446173)

[4.2 Review of Operating System Logs 12](#_Toc73446174)

[4.3 Review of Database Audit Logs 12](#_Toc73446175)

[4.4 Log Retention 12](#_Toc73446176)

[4.5 Windows Machine Monitoring and Logging 13](#_Toc73446177)

[5.0 Business Continuity 19](#_Toc73446178)

[6.0 Incident Management 26](#_Toc73446179)

[6.1 Principles and Basic Concepts 26](#_Toc73446180)

[6.2 Process Scope 26](#_Toc73446181)

[6.3 Process Objectives 27](#_Toc73446182)

[6.4 Policies 27](#_Toc73446183)

[6.5 Roles and Responsibilities 27](#_Toc73446184)

[6.6 Incident Intake Channels 30](#_Toc73446185)

[6.7 Incident Management Lifecycle 30](#_Toc73446186)

[6.8 Incident States in ServiceNow 31](#_Toc73446187)

[6.9 Incident Identification and Classification 33](#_Toc73446188)

[6.10 Initial Support 35](#_Toc73446189)

[6.11 Investigation and Diagnosis 36](#_Toc73446190)

[6.12 Resolution and Recover 37](#_Toc73446191)

[6.13 Incident Closure 39](#_Toc73446192)

[6.14 RACI Matrix 40](#_Toc73446193)

[6.15 Major Incident Management 40](#_Toc73446194)

[6.16 Non-Technical Urgent Issues 42](#_Toc73446195)

[6.17 Incident Candidates 44](#_Toc73446196)

[6.18 Incident Communication Plan 45](#_Toc73446197)

[6.19 Major Incident Reviews 46](#_Toc73446198)

[6.20 Relationship with Other Processes 46](#_Toc73446199)

[7.0 Change Control Process 48](#_Toc73446200)

[7.1 Principles and Basic Concepts 48](#_Toc73446201)

[7.2 Process Description 48](#_Toc73446202)

[7.3 Process Goal and Objectives 48](#_Toc73446203)

[7.4 Policies 49](#_Toc73446204)

[7.5 Process Scope 49](#_Toc73446205)

[7.6 Methods of Raising an RFC 50](#_Toc73446206)

[7.7 Change Types 50](#_Toc73446207)

[7.8. Standard Changes 52](#_Toc73446208)

[7.9 Normal Changes 52](#_Toc73446209)

[7.9.1 Normal Minor 52](#_Toc73446210)

[7.9.2 Normal Significant 54](#_Toc73446211)

[7.9.3 Normal Expedited 55](#_Toc73446212)

[7.10 Emergency Change 55](#_Toc73446213)

[7.11 Change State (ServiceNow) 56](#_Toc73446214)

[7.12 Change Collision 56](#_Toc73446215)

[7.13 Change Calendar 57](#_Toc73446216)

[7.14 Blackout Window 57](#_Toc73446217)

[7.15 Maintenance Window 57](#_Toc73446218)

[7.16 Change Assessment and Evaluation 57](#_Toc73446219)

[7.28 Change Impact Analysis 58](#_Toc73446220)

[7.29 Change Risk Assessment 58](#_Toc73446221)

[7.30 Change Process Roles and Responsibilities 58](#_Toc73446222)

[7.31 RACI Matrix 62](#_Toc73446223)

[7.32 Change Management Process Activities 64](#_Toc73446224)

[7.33 Normal Change: Planning and Submission 66](#_Toc73446225)

[7.34 Normal Change: Assessment 66](#_Toc73446226)

[7.35 Normal Change: Authorization and Scheduling 67](#_Toc73446227)

[7.36 Normal Change: Implementation 68](#_Toc73446228)

[7.37 Normal Change: Review and Closure 68](#_Toc73446229)

[7.38 Emergency Change 70](#_Toc73446230)

[7.38.1 Emergency Change: Planning and Submission 70](#_Toc73446231)

[7.38.2 Emergency Change: Authorization and Scheduling 70](#_Toc73446232)

[7.38.3 Emergency Change: Implementation 70](#_Toc73446233)

[7.38.4 Emergency Change: Review and Closure 72](#_Toc73446234)

[7.39 Standard Change 72](#_Toc73446235)

[7.39.1 Standard Change: Planning and Submission 72](#_Toc73446236)

[7.39.2 Standard Change: Implementation 73](#_Toc73446237)

[7.39.3 Standard Change: Review and Closure 73](#_Toc73446238)

[8.0 Configuration Management 94](#_Toc73446239)

[8.1 Version control 94](#_Toc73446240)

[8.2 Configuration Control Process 95](#_Toc73446241)

[8.3 Configuration Management Database (CMDB) 95](#_Toc73446242)

[8.4 Logical Access Restrictions 95](#_Toc73446243)

[9.0 Solution Design Document 96](#_Toc73446244)

[10.0 User Access 96](#_Toc73446245)

[10.1 User Password Policy 96](#_Toc73446246)

[10.2 User Login Security Rules 99](#_Toc73446247)

[10.3 User Password Recovery 99](#_Toc73446248)

[10.4 User Termination Reports 100](#_Toc73446249)

[10.5 User Inactivity 100](#_Toc73446250)

[10.6 Privileged Access 100](#_Toc73446251)

[10.7 User Access Review 100](#_Toc73446252)

[11. Operational Maintenance 101](#_Toc73446253)

[11.1 Daily Tasks 101](#_Toc73446254)

[11.2 Maintenance Test and Diagnostic Tools 102](#_Toc73446255)

[12. Operational Activities 103](#_Toc73446256)

[12.1 Daily Tasks 103](#_Toc73446257)

[12.2 Weekly Tasks 103](#_Toc73446258)

[12.3 Monthly Tasks 103](#_Toc73446259)

[12.4 Quarterly Tasks 104](#_Toc73446260)

[12.5 Yearly Tasks 105](#_Toc73446261)

[13.0 Vendor O&M 106](#_Toc73446262)

[13.2 Vendor Incident Response Time 107](#_Toc73446263)

[14.0 Document Maintenance 108](#_Toc73446264)

[Appendices 109](#_Toc73446265)

[Appendix A: P1 Escalation List 109](#_Toc73446266)

[Appendix B: P2 Escalation List 109](#_Toc73446267)

[Appendix C: P3 Escalation List 109](#_Toc73446268)

[Appendix D: P4 Escalation List 109](#_Toc73446269)

[Appendix E: Contact List 109](#_Toc73446270)

[Appendix F: Log Review Form 110](#_Toc73446271)

[Appendix G: Server Daily Backup Check 110](#_Toc73446272)

[Appendix H: Database Daily Backup Check 112](#_Toc73446273)

[Appendix I: Filestore Daily Backup Check 113](#_Toc73446274)

[Appendix J: User Role and Active Directory Security Group 113](#_Toc73446275)

[Appendix K: Software Approved List 113](#_Toc73446276)

[Appendix L: Authorized Maintenance Personnel 114](#_Toc73446277)

[Appendix M: Vendor POC List 114](#_Toc73446278)

[Appendix N: Change Roles 114](#_Toc73446279)

**Procedure Table**

|  |  |
| --- | --- |
| **Number** | **Procedure** |
| Procedure 4.1 | Windows Monitoring Agent Install |
| Procedure 4.2 | Windows Logging Agent Install |
| Procedure 4.3 | Windows Tanium Agent Install |
| Procedure 4.4 | Linux Tanium Agent Install |
| Procedure 4.5 | Linux Splunk Agent Install |
| Procedure 4.6 | Linux McAfee Software Installation |
| Procedure 4.7 | Windows McAfee Software Installation |
| Procedure 4.8 | Tenable Windows Software Installation |
| Procedure 4.9 | Tenable Linux Software Installation |
| Procedure 5.1 | Configuring Scheduled VM Backup |
| Procedure 5.2 | Configured Scheduled Backup |
| Procedure 5.3 | Configured Scheduled Filestore Backup |
| Procedure 5.4 | Backup Validation Process |
| Procedure 5.5 | Restore Process |
| Procedure 5.6 | Blue Prism Application Backup Process |
| Procedure 5.7 | Blue Prism Database Backup Process |
| Procedure 5.8 | Blue Prism Application Server Restore Process |
| Procedure 5.9 | Blue Prism Database Server Restore Process |
| Procedure 5.10 | Blue Prism Database Server Scheduling Process |
| Procedure 6.1 | Incident Response Process |
| Procedure 7.1 | Detailed User Creation Change Request |
| Procedure 7.2 | GCP User Creation Change Request |
| Procedure 7.3 | Magneto User Creation Change Request |
| Procedure 7.4 | Windows User Creation Change Request |
| Procedure 7.5 | Rollback Change Request |
| Procedure 7.6 | User Termination Change Request |
| Procedure 7.7 | Patching/Updates Process |
| Procedure 7.8 | Configuration Change Process |
| Procedure 7.9 | Software Installation Request |
| Procedure 7.10 | Client Software Installation |
| Procedure 7.11 | Post Implementation Process |
| Procedure 10.1 | GCP Password Recovery Process |
| Procedure 10.2 | GCP Password Recovery Process – Admin Steps |
| Procedure 11.1.1 | Daily Operational Testing Process |
| Procedure 11.1.2 | Execute Backup Validate Process |
| Procedure 12.1.2 | Daily Stale Accounts Process |
| Procedure 12.3.1 | Review Admin Accounts Process |
| Procedure 12.4.1 | Review Authorized Software List |
| Procedure 12.5.1 | Review Access Agreements Process |
| Procedure 12.5.2 | Review Exceptions to the Traffic Flow policy |
| Procedure 13.1 | Vendor Incident Process |

# Introduction

#### 

## 1.1 D2C2 Program

Amid changing competitive dynamics, heightened demand, and a lack of contact center solutions that truly integrate future technology and the human experience, Deloitte, Google, and Cisco have partnered to create a unique market offering that is first of its type and addresses core needs across all customer segments. Our platform reimagines the contact center with a suite of best-in-class capabilities. We are also putting the customer at the forefront of designing contact centers as a service. Through this world-class, integrated platform, we will disrupt the market by delivering the only FedRAMP-certified, Google CCAI-enabled contact center platform and subsequently position our firms to rapidly expand across various sectors. We will be able to sell our solution to our clients at a competitive cost, positioning us to capture part of a $13.17B market.

## 1.2 Purpose

The NOC SOP (SOP) provides guidance and documentation on the Operations of the NOC, including Environment Monitoring, Incident Response, Change Management, Configuration Management, and related communication efforts. These procedures drive responses to all incidents, including issues whose severity is such that it can affect the ability of the system to do business and undermine its reputation. The NOC must be prepared to deal with these incidents as soon as they occur. The NOC SOP will identify the process and personnel that will be required to mitigate these incidents.

This SOP details the type of monitoring, detection, action, and reporting that is required to adequately protect our infrastructure, data and provide business continuity.

This NOC SOP is intended to provide guidance necessary to:

* + - Quickly and efficiently recover from incidents.
    - Minimize disruption of critical information system and services when incidents occur.
    - Emphasize the need to respond systematically. Following established procedures will increase the likelihood that personnel will carry out all necessary steps to handle an incident correctly.
    - Protect system infrastructure and interrelated systems.
    - Promote efficient use of resources. Ensuring that both technical and managerial personnel respond to an incident requires substantial resources. These resources could be devoted elsewhere if an incident were short-lived. Therefore, resolving the incident as quickly as possible is a high priority.

# Stakeholders

The NOC SOP will be coordinated with the following stakeholders:

* Change Control Board
* Emergency Change Approval Team

# Roles and Responsibilities

## 

This section describes the Incident Response roles and responsibilities of different individuals within the system user and organizational structure. Each individual, from end-user personnel to the Authorizing Official (AO), has responsibilities relating to reportable incidents. It is important, therefore, that all personnel understand their roles and responsibilities in relation to this organization.

## 3.1 Chief Information Security Officer (CISO)

The CISO has the responsibility to report incident information in a timely fashion. In addition, the CISO should be prepared to advise security personnel on immediate response decisions in the event of a serious breach of sensitive information. It is also the CISO’s responsibility to coordinate incoming information, advise users on handling security incidents, and disseminate information to the appropriate personnel.

## 3.2 Project Chief Engineer

The Project Chief Engineer will be the technical lead of the project and will be responsible for all technical decisions. They will also act as the second level approver for change request and approve any rollbacks.

**3.3 Network Operations Center Manager (NOC-M)**

The NOC Manager will be responsible for monitoring the service requests tickets entering the help desk. They will also approve any rollbacks.

**3.4 Shift Manager**

Oversees incidents with a sense of urgency while following standard operating procedures. Assist staff with troubleshooting and resolving common and escalated issues.

## 3.5 Product SME

The Product SME is the first level approver for all change requests.

## 3.6 System Administrator (SA)

The System Administrators are responsible for troubleshooting, defining the scale of the incident, preserving evidence, executing the recovery operations and documenting the actions taken.

## 3.7 End-User

System end-users are usually the most effective in discovering intrusions. Despite advances in intrusion detection systems, most information system incidents are detected by the end users, not by centralized technical measures. End-users must, therefore, be vigilant concerning unusual system behavior that may indicate a security incident in progress. If a computer security incident is detected, they should immediately contact the NOC helpdesk.

# Monitoring

The monitoring process will allow us to observe and capture data pertaining to our infrastructure, in efforts to make informed decisions on our performance and prevent potential incidents.

## 4.1 Incident Error Log Reviews

The log review process outlines the steps required to review the error logs of all system components related to an incident. The following components include:

* Operating System Logs
* Database Audit Logs
* Application Logs
* Google Logging entries from Google services

## 4.2 Review of Operating System Logs

Operating System Log events are sent to the Google Cloud Logging system.

## 4.3 Review of Database Audit Logs

Database events are sent to the Google Cloud Logging system.

## 4.4 Log Retention

Logs will be retained for a minimum of 13 months.

## 4.5 Windows Machine Monitoring and Logging

**Procedure 4.5.1 – Windows Monitoring Agent Install**

**Frequency:** Upon initial windows machine creation

**Description:** The Windows Monitoring Install procedure outlines the steps taken to install monitoring agents on all Windows machines.

**Prerequisites:** Production Windows machines

**Targets:** Windows machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Copy the contents of the project service account.json to this file (either copy the accompanying file to the folder specified and then rename it, or create a new file and copy the contents in)  C:\ProgramData\Google\Auth\application\_default\_credentials.json  You will (probably) have to create the directory structure as well | See accompanying file for each project |
| 2. | Set the environment variable: GOOGLE\_APPLICATION\_CREDENTIALS  To equal this:  C:\ProgramData\Google\Auth\application\_default\_credentials.json | Easiest way – click on start – type advanced system settings – click on environment variables – then click new under system variables |
| 3. | Switch to home directory | Cd~ |
| 4. | Open Admin PowerShell prompt and copy this: | (New-Object Net.WebClient).DownloadFile(“<https://repo.stackdriver.com/windows/StackdriverMonitoring-GCM-46.exe>”, “${env:UserProfile}\StackdriverMonitoring-GCM-46.exe”) & “{env:UserProfile}\StackdriverMonitoring-GCM-46.exe” |
| 5. | Check and see if the service is running – you should see the Name, DisplayName and the status, which should show running | get-service StackdriverMonitoring |

**Procedure 4.5.2 – Windows Logging Agent Install**

**Frequency:** Upon initial windows machine creation

**Description:** The Windows Logging Install procedure outlines the steps taken to install logging agents on all Windows machines.

**Prerequisites:** Production Windows machines

**Targets:** Windows machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Open up PowerShell admin and switch to your home directory | Cd~ |
| 2. | Paste into the PowerShell command line | (New-Object Net.WebClient).DownloadFile(<https://dl.google.com/cloudagents/windows/StackdriverLogging-v1-14.exe>”, “${env:UserProfile}\StackdriverLogging-v1-14.exe”) |
| 3. | Paste into the PowerShell command line and validate a registry key is returned | Reg query  HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\GoogleStackdriverLoggingAgent\/vVersion |
| 4. | Check and see if the service is running – you should see the Name, DisplayName and the status which should show running | get-service StackdriverLogging |

**Procedure 4.5.3 – Windows Tanium Agent Install**

**Frequency:** Upon initial windows machine creation

**Description:** The Windows Tanium Install procedure outlines the steps taken to install Tanium monitoring agents on all Windows machines.

**Prerequisites:** Production Windows machines

**Targets:** Windows machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Open up PowerShell admin and switch to your home directory | Cd~ |
| 2. | Paste into the PowerShell command line | SetupClient.exe /ServerAddress=usfed95063.deloittefed.com,usfed95064.deloittefed.com,10.6.95.63,10.6.95.64 /ServerPort=17472 /KeyPath=”anita-init.dat” /S |
| 3. | In some cases you have to use the absolute path to the key, for example: | SetupClient.exe /ServerAddress=usfed95063.deloittefed.com,usfed95064.deloittefed.com,10.6.95.63,10.6.95.64 /ServerPort=17472 /KeyPath=”C:\KEY\tanium-init.dat” /S |
| 4. | Start the service: | net start “Tanium Client” |
| 5. | Check that it is running: | sc query “Tanium Client” |

**Procedure 4.5.4 – Linux Tanium Agent Install**

**Frequency**: Upon initial Linux machine creation

**Description:** The Linux Tanium Install procedure outlines the steps taken to install Tanium monitoring agents on all Linux machines.

**Prerequisites:** Production Linux machines

**Targets:** Linux machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Open up PowerShell admin and switch to your home directory | Cd~ |
| 2. | Paste into the PowerShell command line | **For RedHat 8:** rpm -I TaniumClient-7.4.4.1250-1.rhe8.x86\_64.rpm  **For RedHat 7**: rpm -I TaniumClient-7.4.4.1250-1.rhe7.x86\_64.rpm |
| 3. | After successful installation, you need to run the following commands: | 1. cp anita-init.dat /opt/Tanium/TaniumClient/ 2. /opt/Tanium/TaniumClient/TaniumClient config set ServerAddress usfed95063.deloittefed.com,usfed95064.deloittefed.com,10.6.95.63,10.6.95.64 3. /opt/Tanium/TaniumClient/TaniumClient config set ServerPort 17472 4. /opt/Tanium/TaniumClient/TaniumClient config set KeyPath /opt/Tanium/TaniumClient/TaniumClient/anita-init.dat |
| 4. | Start the service: | systemctl start taniumclient.service |
| 5. | Check that it is running: | systemctl status taniumclient.service |

**Procedure 4.5.5 – Linux Splunk Agent Install**

**Frequency:** Upon initial Linux machine creation

**Description:** The Linux Splunk Install procedure outlines the steps taken to install Splunk monitoring agents on all Linux machines.

**Prerequisites:** Production Linux machines

**Targets:** Linux machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Create the following directories as ROOT: | **/tmp/UF/Global\_Fusion\_Center\_Splunk\_UF\_7.3.3.0x64\_linux** |
| 2. | Install all the related files for Linux into the “**Global\_Fusion\_Center\_Splunk\_UF\_7.3.3.0x64\_linux**”directory |  |
| 3. | Run: | **chmod +x splunk\_UF\_Linux-x86\_64\_install.sh** |
| 4. | Run the installation: | **./splunk\_UF\_Linux-x86\_64\_install.sh “USGPS”** |
| 5. | Update the nameserver | This allows us to communicate with the Splunk DNS |
| 6. | As the ROOT, create the **/etc/NetworkManager/conf.d/90-dns-none.conf** file with this in it:  **[main]**  **dns=none** |  |
| 7. | Save and then reload the NetworkManager: **systemctl reload NetworkManager** |  |
| 8. | Go and edit the **resolv.conf** file: **/etc/resolv.conf** (You can leave additional information at the top, just need to update the nameservers to below information)  **nameserver 10.100.12.10**  **nameserver 10.200.12.10** |  |
| 9. | Save and reload the NetworkManager again: **systemctl reload NetworkManager** |  |
| 10. | Verify that the **resolv.conf** file didn’t override your changes |  |

**Procedure 4.5.6 – Linux McAfee Software Installation**

**Description:** The Linux McAfee Software Installation procedure outlines the steps needed in order to install McAfee software on our Linux machines.

**Frequency**: Upon creation of a new Linux machine

**Prerequisites:**

1. Approved Software Installation request
2. The agent extension must be installed on McAfee ePO and appropriate agent packages added to the Master Repository before the agent can be installed onto a non-Windows system

**Targets:** Linux Machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Select **Menu** |  |
| 2. | Select **Systems** |  |
| 3. | Select **System Tree** |  |
| 4. | Click **New Systems** |  |
| 5. | Select **Create and download agent installation package** |  |
| 6. | Choose the appropriate **Agent Version** |  |
| 7. | Click **OK** | Save the agentPackages.zip file that contains the install.sh file. |
| 8. | Open **Terminal**, then switch to the location where you copied the install.sh file |  |
| 9. | Run these commands, giving root credentials when requested: | sudo chmod +x install.sh  sudo ./install.sh -i |

**Procedure 4.5.7 – Windows McAfee Software Installation**

**Description:** The Windows McAfee Software Installation procedure outlines the steps needed in order to install McAfee software on our Windows machines.

**Frequency**: Upon creation of a new Windows machine

**Prerequisites:**

1. Approved Software Installation request
2. McAfee Agent extension must be installed on McAfee ePO and appropriate software and key updater packages must be added to the Master Repository.

**Targets:** Windows Machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Select **Menu** |  |
| 2. | Select **Systems** |  |
| 3. | Select **System Tree** |  |
| 4. | Click **Actions** > **Agent** > **Deploy Agents** |  |
| 5. | Select the appropriate **Agent Version** drop-down list, given the target operating system, and select a version from that list. |  |
| 6. | Select these options as appropriate:   * Install only on systems that do not already have an agent managed by this McAfee ePO server * Force installation over existing version | Note: if you use force installation option, the existing McAfee Agent is removed in its entirety, including policies, tasks, events, and logs, before the new McAfee Agent is installed. |
| 7. | To change the installation path from the default, enter the target path in the **Installation Path** option. |  |
| 8. | Type valid credentials in the **Domain**, **Username**, and **Password** and **Confirm Password** fields. | If you want these entries to be the default for future deployments, select **Remember my credentials for future deployments**. |
| 9. | If you do not want the default values, enter values in the **Number of attempts, Retry interval**, and Cancel after options |  |
| 10. | If you want the deployment to use a specific Agent Handler, select it from the drop-down list. If not, select **All Agent Handlers**. |  |
| 11. | Click **OK** | The **Server Task Log** page appears with the **Deploy McAfee Agent** task listed. |

**Procedure 4.5.8 – Tenable Windows Software Installation**

**Description:** The Tenable Windows Software Installation procedure outlines the steps needed in order to install Tenable software on our Windows machines.

**Frequency**: Upon creation of a new Windows machine

**Prerequisites:**

1. Approved Software Installation request

**Targets:** Windows Machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Get an installer from [Nessus Agent Download page](https://www.tenable.com/agent-download) | Download either:  NessusAgent-8.2.4-64.msi  NessusAgent-8.2.4-Win32.msi |
| 2. | Navigate to the folder where you downloaded the Nessus installer |  |
| 3. | Next, double click the file name to start the installation process |  |
| 4. | First, the **Welcome to the InstallShield Wizard for Tenable, Inc. Nessus** screen appears. Select **Next** to continue |  |
| 5. | Select the **I accept the terms of the license agreement** option, and then click **Next** |  |
| 6. | On the **Destination Folder** screen, select the **Next** button to accept the default installation folder. Otherwise, select the **Change** button to install Nessus to a different folder. |  |
| 7. | On the **Ready to Install the Program** screen, select the **Install** button |  |
| 8. | The **Installing Tenable, Inc. Nessus** screen will be displayed and a **Status** indication bar will illustrate the installation progress. | The progress may take several minutes |
| 9. | Has WinPcap been installed previously? |  |
| 9.1 | If Yes: continue with installation  If No: system will present Install WinPcap. | Follow WinPcap procedures to install. |
| 9.2 | On the **Welcome to the WinPcap Setup Wizard** screen, select the **Next** button. |  |
| 9.3 | On the **WinPcap Lincense Agreement screen**, read the terms of the license agreement, and then select the **I Agree** button to continue. |  |
| 9.4 | On the **WinPcap installation options** screen, ensure that the **Automatically start the WinPcap driver at boot time** option is checked, and then select the **install** button. |  |
| 9.5 | On the **Completing the WinPcap Setup Wizard** screen, select the **Finish** button. The **Tenable Nessus InstallShield Wizard Completed** screen appears |  |
| 9.6 | Select the **Finish** button |  |
| 10. | After the **InstallShield Wizard** completes, the **Welcome to Nessus** page loads in your default browser |  |

**Procedure 4.5.9 – Tenable Linux Software Installation**

**Description:** The Tenable Linux Software Installation procedure outlines the steps needed in order to install Tenable software on our Linux machines.

**Frequency**: Upon creation of new Linux machines

**Prerequisites:**

1. Approved Software Installation request

**Targets:** Linux Machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Get an installer from [Nessus Agent Download page](https://www.tenable.com/agent-download) | Download either: |
| 2. | From a command prompt, run the Nessus install command specific to your operating system. | # rpm -ivh Nessus-<version number>-es6.x86\_64.rpm |
| 3. | Start the Nessus Daemon |  |
| 3.1 | From a command prompt, restart the nessusd daemon | # service nessusd start |

# Business Continuity

The business continuity process will allow us to continue to deliver our services at acceptable levels should a disruptive incident occur. Continuity and resilience are of paramount importance; therefore, our prevention and recovery process will deal with potential threats to our systems in order to enable ongoing operations.

Key factors that will be incorporated into our business continuity process are:

* + **Multi location strategy** – Applications are based upon services, processes, and virtual machines that are located in multiple geographic locations to ensure the loss of a location or a process will not negatively impact availability. Where possible, load balancers provide access to the active parts of the solution and assist in failover.
  + **Snapshots** – We perform nightly backups of servers which allow for point in time complete restoration.
  + **Filestore backup –** we perform nightly backups of filestore locations to ensure key data is available for a point in time restoration.
  + **Cloud storage backups –** we perform nightly backups of cloud storage to ensure key data is available for a point in time restoration.
  + **Database backups –** we perform nightly backups of databases to filestore locations to ensure databases can be recovered when required.
  + **Recovery process –** detailed recovery procedures are documented and tested for restoring all applications, services, processes, and virtual machines in the event of a disaster.

**Procedure 5.1 – Configuring scheduled VM Backup**

**Frequency:** Upon initial VM creation.

**Description:** The Virtual Machine Backup procedure will allow us to schedule nightly snapshots of our production VMs so that we have backups to restore from in the case of a disaster.

**Prerequisites:** Production VMs

**Targets:** Servers listed in Appendix G.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Login to the Google GCP Console |  |
| 2. | Select **VM Instances** |  |
| 3. | Select **Snapshot** |  |
| 4. | Create **Snapshot** |  |
| 5. | Name **Snapshot** |  |
| 6. | Select **Source Disk** |  |
| 7. | Location set to **Multi-Region** |  |
| 8. | Go to **Create a Snapshot Schedule** |  |
| 9. | Schedule snapshots to be run **Daily** |  |
| 10. | Enter Start time to 11pm EST |  |
| 11. | Enable VSS |  |
| 12. | Select **Keep Snapshot** |  |
| 13. | Assign snapshot |  |
| 14. | Go to **VM Instances** |  |
| 15. | Select **Instance to Assign** |  |
| 16. | Go to **Disk** |  |
| 16.1 | Click on the **Disk** |  |
| 16.2 | **Edit** |  |
| 16.3 | Snapshot Schedule – Select the one that was created |  |
| 16.4 | **Save** |  |

**Procedure 5.2 – Configured Scheduled Backup**

**Frequency:** Upon initial database creation

**Description:** The Database Backup procedure will allow us to take a backup of our databases into Google filestore nightly so that we may have data to restore from in the case of a disaster.

**Prerequisites:** Active databases

**Targets:** Databases listed in Appendix H.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Configure nightly job to execute backup batch file |  |
| 2. | Create backup batch file to contain MySQL dump command | mysqldump –all-databases > <insert filestore path> dump.sql |
| 3. | Execute test backup to confirm it works |  |

**Procedure 5.3 – Configured Scheduled Filestore Backup**

**Frequency:** Upon initial filestore creation

**Description:** The Filestore Backup procedure will allow us to backup all filestore locations used by applications. This will be done nightly so that we may have data to restore from in the case of a disaster.

**Prerequisites:** Application servers

**Targets:** Servers listed in Appendix G.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Go to the Filestore instance page |  |
| 2. | Click **Create Backup** |  |
| 3. | For **Backup ID**, type a name for the backup | * Include two letters of the application * Year/Month/Day e.g. 20210524 * Filestore * e.g., lk-20210524-filestore |
| 4. | For **Region**, select the Google Could region where you want the backup to be located | Make sure to back it up to two regions (e.g., East and West) |
| 5. | Click **Create** |  |

**Procedure 5.4 – Backup Validation Process**

**Description:** The Backup Validation procedure will allow us to validate that each backup was successfully completed. This will be done daily so that we may ensure backups were executed correctly.

**Frequency:** Daily

**Prerequisites:**

1. Snapshots executed nightly for all virtual machines (VMs)
2. Database backups performed nightly
3. Scheduled jobs are configured

**Targets:** VMs listed in Appendix G, Databases listed in Appendix H, Application listed in Appendix G.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Check VM snapshots from production suite |  |
| 1.1 | Log into Google console |  |
| 1.2 | Navigate to **snapshot location** | Compute Engine > Snapshots |
| 1.3 | Validate snapshot date, time and file size for each server |  |
| 2 | Validate each database backup |  |
| 2.1 | Navigate to **Filestore** | Storage>Filestore>Backups |
| 2.2 | Go to **Backups Tab** |  |
| 2.3 | Validate database backup file, file size, file date and time |  |
| 3 | Validate file store has successfully backed up |  |
| 3.1 | Click on F**iletore link** |  |
| 3.2 | Go to **Backups Tab** |  |
| 3.3 | Validate filestore backup date and time |  |

**Procedure 5.5 – Restore Process**

**Description:** The Restore procedure will allow us to restore our servers and databases back to a specific point in time in the event of a disaster.

**Frequency:** Whenever we experience a failure that requires a system restore.

**Prerequisites:**

1. New data center/zone identified for recovery location
2. VPC and subnets are accessible from new recovery location
3. Snapshots for all virtual machines (VMs) validated
4. Database backups validated
5. Filestore backup validated

**Targets:** VMs listed in Appendix G, Databases listed in Appendix H, Application listed in Appendix G.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Restore each server in recovery locations | Repeat per server required for the application (see list of servers in Appendix G) |
| 2. | Restore all filestores |  |
| 3. | Restore all cloud storage buckets | Only if issues with multi-region buckets |
| 4. | Restore all databases |  |

**Procedure 5.6 – Blue Prism Application Backup Process**

**Description:** The Blue Prism Application Backup procedure will allow us to back up the Blue Prism application servers.

**Frequency:** Upon initial Blue Prism application server creation.

**Prerequisites:** Active Blue Prism application servers.

**Targets:** Blue Prism application servers.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Take a copy of the folder structure and \*.bpk files in the configured location. |  |
| 2. | Take a copy of automate.config located here C:\ProgramData\Blue Prism Limited\Automate V3 |  |

**Procedure 5.7 – Blue Prism Database Backup Process**

**Description:** The Blue Prism Database Backup procedure will allow us to back up the Blue Prism database servers.

**Frequency:** Upon initial Blue Prism database server creation.

**Prerequisites:** Active Blue Prism database servers.

**Targets:** Blue Prism database servers.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | After connecting to the appropriate instance of the Microsoft SQL Server Database Engine, in **Object Explorer**, expand the server tree |  |
| 2. | Expand **Databases**, and either select a user database or expand **System Databases** and select a system database |  |
| 3. | Right-click the database that you wish to backup (bp-magnetohealth01), point to **Tasks**, and then click **Back Up** |  |
| 4. | In the **Back Up Database** dialog box, the database that you selected appears in the drop-down list | Which you can change to any other database on the server |
| 5. | In the **Backup type** drop-down list, select the desired backup type – the default is **Full**. |  |
| 6. | Under **Backup component**, select **Database** |  |
| 7. | **Destination** section, review the default location for the backup file (in the ../mssql/data folder) |  |
| 8. | Click **OK** to initiate the backup |  |
| 9. | When the backup completes successfully, click **OK** to close the SQL Server Management Studio dialog box |  |

**Procedure 5.8 – Blue Prism Application Server Restore Process**

**Description:** The Blue Prism Application Server Restore procedure will allow us to restore our application servers back to a specific point in time in the event of a disaster.

**Frequency:** Whenever we experience a failure that requires a system restore.

**Prerequisites:** Blue Prism Application servers backup validated.

**Targets:** Blue Prism application servers.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Place the file into the default or custom location  dependent on your configuration. The default location for the Automate.config file is:  C:\ProgramData\Blue Prism Limited\Automate V3 |  |
| 2. | Edit the profile using BPServer.exe and update the  database connection |  |
| 3. | Place encryption scheme information into a selected location that is accessible to the application server and use BPServer.exe to edit the profile and update the  configured location of the stored keys |  |
| 4. | Validate that the encryption scheme information is valid |  |
| 5. | In BPServer.exe validate the settings for the selected connection mode, and disable the Scheduler on this device |  |
| 6. | Set the Blue Prism server service to operate under the selected user context |  |
| 7. | Start the Blue Prism server service |  |
| 8. | Connect the first interactive client to the application server (or database). |  |
| 9. | Create the first runtime resource and connection to the application server (or database) |  |

**Procedure 5.9 – Blue Prism Database Server Restore Process**

**Description:** The Blue Prism Database Server Restore procedure will allow us to restore our database servers back to a specific point in time in the event of a disaster.

**Frequency:** Whenever we experience a failure that requires a system restore.

**Prerequisites:** Blue Prism Database servers backup validated.

**Targets:** Blue Prism Database servers.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Launch SQL Server Management Studio and connect to the SQL Server instance |  |
| 2. | Right-click the **Databases** node in **Object Explorer** and select **Restore Database** |  |
| 3. | Select **Device:**, and then select the ellipses (...) to locate your backup file |  |
| 4. | Select **Add** and navigate to where your .bak file is located. Select the .bak file and then select **OK**. |  |
| 5. | Select **OK** to close the **Select backup devices** dialog box |  |
| 6. | Select **OK** to restore the backup of your database |  |

**Procedure 5.10 – Blue Prism Database Server Scheduling Process**

**Description:** The Blue Prism Database Server scheduling procedure will allow us to schedule the back up of our database servers.

**Frequency:** Daily

**Prerequisites:** Active Blue Prism database servers.

**Targets:** Blue Prism Database servers.

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Launch Microsoft SQL Server Manager |  |
| 2. | Connect to the server and instance that the database(s) were installed to |  |
| 3. | Expand the folder called “Management” |  |
| 4. | Right click the folder called “Maintenance Plans” |  |
| 5. | Select Maintenance Plan Wizard |  |
| 6. | If you receive the SQL Server Maintenance Plan Wizard splash screen, click “Next |  |
| 7. | On the Select Plan Properties screen, do the following:   * Change the Name field to state “Backup” * Click the “Change” button * Change the Frequency Settings to “Occurs Daily and Recurs every 1 day”. * Set the Daily frequency to “Occurs once at 12:00:00 AM”. * Set the Duration start date to “today”. * Set the end date to “No end date”. * Click “OK”. |  |

# Incident Management

## 6.1 Principles and Basic Concepts

An incident is defined as an unplanned interruption or a reduction in the quality of a technical service or a failure of a Configuration Item (CI) that has not yet impacted a technical service. Incidents can include failures or degradation of services reported by users, technical staff, third-party suppliers and partners, or automatically from monitoring tools.

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact of incidents on business operations, ensuring that the best possible levels of service quality and availability are maintained. Normal service operation is defined as an operational state where services and CIs are performing within agreed service and operational levels. Incident management is responsible for managing the lifecycle of all incidents. A temporary workaround to restore service is all that is required in many cases to complete the process.

ServiceNow focuses on the use of automation and information to speed the path to resolution.

Incident Management relies heavily on:

* The Configuration Management process for incident assignment and impact analysis
* The Problem Management process for the investigating root causes of incidents and providing workarounds and permanent resolutions
* The Change Management process for controlling changes needed to resolve incidents and minimizing incidents caused by change

## 6.2 Process Scope

The scope of Incident Management includes:

* The identification and diagnosis of incidents through Event Management, technical identification and user reports
* The resolution of all incidents as quickly as possible using:
  + - Defined resolution processes
    - Problem Management identified Known Errors (workarounds)
    - Identifying new resolution activities through diagnosis
* Identifying incidents and groups of incidents that require further analysis in the Problem Management process for elimination or reduction in resolution time
* Incident resolution is aligned to business need by prioritizing activities through defined service levels and objectives agreed to in consultation with the business
* Incident records should be audited on a regular basis to ensure they have been categorized correctly and includes the information needed to enable incident resolution activities on the part of all support groups. The results of the audit and recommendations on the resolution of audit issues should be communicated to Incident Managers
* A common set of criteria for prioritizing and escalating incidents, agreed to by both IT and the business, should be established in advance and well communicated
* Where possible, automation will be leveraged to route and resolve incidents without human intervention

## 6.3 Process Objectives

The objectives of Incident Management are to:

* Ensure standard methods and procedures are used for efficient and prompt incident response, analysis, documentation, management, and reporting
* Increase visibility and communication of incidents to business and support staff
* Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
* Align Incident Management activities and priorities with those of the business
* Maintain user satisfaction with the quality of IT services

## 6.4 Policies

Incident management policies are required to guide all staff in the behaviors needed to make incident management effective. Policy statements are be based on the IT Service Management strategy and overarching IT policies.

The following are the Incident Management policies.

* Customer satisfaction with the Incident Management Process must be maintained at all times by staffing adequate customer-oriented and technically trained support staff with the correct skill levels and effectively utilizing resources at all stages of the process
* Ensure standard methods and procedures are used for efficient and prompt incident response, analysis, documentation, management, and reporting
* Increase visibility and communication of incidents to business and support staff
* Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
* Align Incident Management activities and priorities with those of the business
* Maintain user satisfaction with the quality of IT services
* Where possible, automation should be leveraged as a means to resolve incidents without human intervention

## 6.5 Roles and Responsibilities

Each role is assigned to perform specific tasks within the process. Within a specific process, there can be more than one individual associated with a specific role. Additionally, a single individual can assume more than one role within the process although typically not at the same time. Depending on the structure and maturity of a process, all roles described may not exist in the current IT organization.

The following describes the roles defined for Incident Management.

|  |  |
| --- | --- |
| Role | Description |
| Caller/End User | * Report incidents to NOC Help Desk * Participate in the implementation of a solution or workaround * Confirm successful resolution * Provide feedback on and acceptance of identified resolutions or workarounds * Provide feedback on Services received via incident survey |
| NOC Help Desk Agent (1St Level) | * Record, own, monitor, track, and communicate about incidents * Single point of contact (SPOC) for end users * Investigate and diagnose incidents * Conduct initial local support (triage) and classification * Provide resolutions and workarounds from standard operating procedures and existing known errors * Escalate incidents to NOC support * Communicate with the caller   The NOC Help Desk Agent is engaged in the process by setting the Assignment Group field to ‘NOC Help Desk’ and the Assigned to field to the individual agent. |
| NOC Support Teams (2nd and 3rd Level) | * Investigate and diagnose incidents escalated from the NOC Help Desk * Develop workarounds * Resolve and recover assigned incidents * Create incidents after detecting a service failure or quality degradation or a situation that may result in one   The NOC Support Team is engaged in the process by changing the Assignment Group field to the support group in question and the Assigned to field to the individual support staff. |
| Incident Manager(s) | * Drive the efficiency and effectiveness of the Incident Management process * Monitor the effectiveness of the Incident Management process and make recommendations for improvement * Execute the Incident Management process with support from individual support groups   Escalates incidents (functional and/or hierarchical) |
| Major Incident Manager(s) | * Co-ordinate the investigation and resolution of major incidents * Assign tasks to other teams to investigate and resolve the major incident * Manage communications during the major incident to technical, business and IT stakeholders * Conduct a review of the major incident once resolved   The Major Incident Manager is engaged in the process by changing the Assignment group field to the Major Incident Management group and the Assigned to field to the correct Major Incident Manager |
| Process Owner | * Define the overall mission of the process * Establish and communicate the process mission, goals, and objectives to all stakeholders * Document and maintain the process and related procedures * Ensure proper staffing and training for execution * Direct the Incident Management roles * Ensure consistent execution of the process across the organization * Monitor, measure, and report on the effectiveness of the process to the leadership * Continually improve the process |

## 6.6 Incident Intake Channels

**6.6.1 Directly in ServiceNow**

The NOC Help Desk Agent can create the incident directly as a result of a phone call or email from a user. A member of NOC Support can raise an incident when they discover evidence of one.

**6.6.2 Incident from a Change**

Any ITIL user can create an incident from a Change when they discover evidence of an issue due to change.

**6.6.3 Automatically via Integrations**

Incidents can be automatically generated via external systems such as event monitoring or direct APIs.

**6.6.4 Call to NOC Help Desk**

End users can call NOC Help Desk at xxx-xxx-xxxx to report an incident.

**6.6.5 Inbound Email**

End users can send emails to [helpdesk@xxx.com](mailto:helpdesk@xxx.com) to generate incident records.

## 6.7 Incident Management Lifecycle

**6.7.1 Process Activities**

|  |  |  |
| --- | --- | --- |
| ID | Activity | Description |
| INC P | Incident Management Planning and Design | * The Incident Management team and key stakeholders decide and document, in the Incident Management section of the NOC SOP, what level of Incident Management is required to support the services delivered by the organization and how this level will be achieved. The planning and design of Incident management depends on Incident intake channels decided, SLA definitions, assignment rules and support levels defined. * This activity is always performed when the process and services are being defined and setup. Additionally, it is good practice to periodically review the Incident Management section to ensure that the process remains relevant to the support needs of the organization and is aligned to Continual Service Improvement. |
| INC 1.0 | Incident Identification and Classification | * Gathering information needed to facilitate service disruption analysis and assignment * Redirecting improperly routed service requests to the request fulfillment process * Determining the incident priority * Associating the incident with a relevant SLA * Invoking the major incident procedure where applicable |
| INC 2.0 | Initial Support | * Matching the incident against other related calls, events, incidents, known errors, or changes that are open or have been recently closed * Escalation to 2nd level support, if necessary * In many cases, corresponding workarounds, known errors, or quick fixes documented in the knowledge base allow incidents to be resolved at 1st level support without recourse to further resources |
| INC 3.0 | Investigation and Diagnosis | * Performing full investigation and diagnosis of the assigned incident * Providing advice on possible workarounds or temporary fixes * Using standard operational procedures and work instructions to ensure that service can be restored as quickly as possible |
| INC 4.0 | Resolution and Recovery | * Restoring the service so that it is available for use * Repairing or replacing the faulty CI(s) * Submitting an RFC when a change is necessary to achieve incident resolution * Informing the customers and users that the service is restored * Verifying with the customer or callers that service restoration is satisfactory |
| INC 5.0 | Incident Closure | * As far as practicable, confirmation that the service is truly restored should be obtained from the caller(s) before the incident is closed * Auto closure of Incidents will happen after 7 calendar days after incident is Resolved |
| INC C | Continual Service Improvement | * Ongoing activities to regularly measure and monitor the efficiency and effectiveness of the process and identify, plan and implement improvements |

## 6.8 Incident States in ServiceNow

States in any ServiceNow application serve a specific purpose. They are designed to make it clear where in a process a record currently resides and to display progress. States should represent a unique phase in a process where a specific set of related activities are grouped together designed to achieve an outcome in order to move to the next phase of the process, Incident Management has the following state model.

* New
* In Progress
* On Hold
* Resolved
* Closed
* Canceled

| Incident Process Area | ServiceNow State | Description |
| --- | --- | --- |
| Identification and Classification | New | When an incident is first created, it is in a state of New. This is where the incident ticket is opened and all known information about the symptoms experienced is captured. Capturing sufficient and relevant detail at this stage is very important |
| Initial Support/Investigation and Diagnosis | In Progress | Auto-assignment will populate the assignment group based on the CI selected. The new assignment group will review the incident arrived in their work list and assign it to an individual to focus on.  Once that individual begins working on the incident, they will manually set the state field to In Progress. Alternatively, the Agent may need to begin some investigation and triage. At this point, they will assign the incident to themselves using the Assigned to field and set the state field to In Progress. It is mandatory to assign an individual to the incident in order for the incident record to move to In Progress. |
| Initial Support/Investigation and Diagnosis | On Hold | The ‘On Hold’ state is used to indicate where an incident is not yet resolved but is temporarily not being worked while waiting for further action to occur outside of the control of the Assigned To individual.  An additional On Hold reason field determines why the incident is on hold. When the ticket is in On Hold state, the resolution SLAs are paused. |
| Resolution and Recovery | Resolved | In order to move the State to Resolved, the Assigned To individual will need to give some further details to explain what the issue was and how it was fixed. The mandatory fields are:   * Resolution code * Resolution notes   The Resolution codes field is a choice list focused on the nature of the resolution provided; for example, whether a workaround was provided or a permanent fix. They are not intended to explain how the incident was resolved. |
| Incident Closure | Closed | No activities take place at this state. Should the incident reoccur a new ticket must be raised. Once an incident is closed, it cannot be reopened. |
| Identification and Classification | Cancelled | There are very few scenarios where an incident is genuinely canceled. This will only occur when an incident was raised in error usually prematurely before realizing there is no real issue. |

## 6.9 Incident Identification and Classification

Capturing enough relevant detail at this stage is very important as it will aid in diagnosis if the incident requires escalation. A description of the incident in the caller’s own words should be recorded so that future contact with the caller considers their understanding of the issue.

| **ID** | **Activity** | **Description** |
| --- | --- | --- |
| INC 1.1 | Log New Incident | Methods of Logging an Incident:   * Directly in ServiceNow * Incident from a Change * Automatically via Integrations * Call to NOC Help Desk * Inbound Email |
| INC 1.2 | Verify User Information | * Gathering information needed to facilitate service disruption analysis and assignment * Redirecting improperly routed service requests to the request fulfillment process * Determining the incident priority * Invoking the major incident process where applicable |
| INC 1.3 | Capture Incident Details | * Select the contact type:   + Email   + Phone * Incident State is automatically set to “New” * Select an available Configuration Item (CI) * Summarize the incident symptoms in the Short Description field * Describe the symptoms of the incident in the Description field:   + What the caller is trying to do   + What is happening   + What actions were taken by the caller   + When did the incident occur?   + Are there any error messages (\*Note – if possible, get a copy of the error message and attach it to the incident record) |
| INC 1.4 | Categorize Incident | * Select the appropriate Category and Subcategory to best categorize the issue |
| INC 1.5 | Prioritize Incident | * Select the appropriate levels of impact and urgency. This drives the prioritization level for the incident |

A description of the incident in the caller’s own words should be recorded so that future contact with the caller can be made in their terms.

The mandatory fields are:

* Caller
* Category
* Sub- Category
* Configuration Item
* Short Description
* Contact Type
* State
* Impact
* Urgency
* Assignment Group

Note: When the User is selected for an Incident, field “Location” is auto populated with date in reference to user which is read only and additional information on Location can be provided in “Additional Location Info” field.

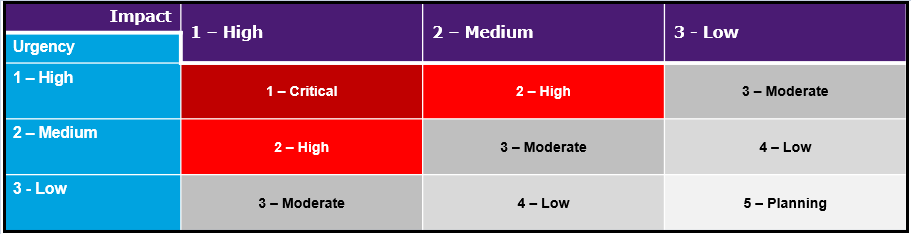
**Establishing Priority**

Incident prioritization typically drives the timeframe associated with the handling of the incident and the time to resolution. This will impact the Service Level Agreements that are associated with the incident. Priority is calculated through a combination of Impact and Urgency.

**Impact** is the affect that an incident has on business. For example, if the incident only impacts a single employee, the impact is low in comparison to 500,000 paying customers with social media accounts.

**Urgency** is the extent to which the incident’s resolution can bear delay.

Priority is generated from urgency and impact according to the following table.



It is possible to automatically establish the priority of the incident based on the CI that is identified in the incident record. With this technique, the business criticality value of the CI is used to determine the priority of the incident.

## 6.10 Initial Support

Initial diagnosis of incidents is largely a human process in most organizations. The NOC Help Desk looks at the information within the incident and communicates with the user to diagnose the source of the service interruption or degradation.

To aid in the process, the agent can consult the configuration management database (CMDB). The CMDB contains information about hardware and software within a network and the relationships between them. The agent can also use IT Knowledge article to aid in quicker diagnosis and resolution of the incident.

The primary focus at this stage is to eliminate unnecessary incident noise, resolve as many true incidents as possible at Level 1 and escalate those than cannot be resolved, quickly, to Level 2.

| **ID** | **Activity** | **Description** |
| --- | --- | --- |
| INC 2.1 | Perform Incident Matching | * Search open incidents with the same user, configuration item and/or categorization to determine if a duplicate incident exists   \*Note: If the affected CI has been identified, open the CI dependency view to determine if there are related incidents that may be causing this issue   * Search open problem and known error records to determine if there are any problems or known errors, with corresponding category and symptoms, that may be related to this incident * Search recent change records to determine if there was a change that may have caused this incident |
| INC 2.2 | Associate Incident to Related Record | Criteria for deciding duplicate Incident is that the Incident reported has same issue description, same CI and requested by same user, then   * Set the incident state to “Canceled” * Save the incident record   In the Related Records section:   * If a related problem or known error record was identified, select the problem number in the “Problem” field * If a related change record was identified, Select the change number in the “Caused by Change” field. Go to INC 2.5 |
| INC 2.3 | Search Knowledge | * Incident record State is updated to “In Progress” * In the Related Search Results of the incident form, review displayed related results and filter them as needed * Select related knowledge as appropriate to link to the incident   If related knowledge does not exist, or a resolution was not identified in selected knowledge, go to INC 2.5 |
| INC 2.4 | Apply Documented Resolution | * Apply solution or documented workaround defined in selected knowledge * If incident is resolved, go to INC 5.0 |
| INC 2.5 | Assign and Update | * If no documented known error or workaround exists or if identified documented resolution did not resolve the incident, select the appropriate assignment group * Update Additional Comments field with customer visible details on resolution progress * Update Work Notes field with details of all activities performed to this point * Save the incident record |

The individual may subsequently reassign the incident to another assignment group or individual if they discover that there is a better-suited group/individual to deal with the issue. This is done by updating the Assignment group and Assigned to fields and may involve passing the incident to 2nd or 3rd line subject matter experts. An email notification will be sent to the new assignees to make them aware they are now responsible.

It is possible for the incident to be reassigned multiple times whilst it is In Progress as different teams may need to be involved. When reassigning an incident, it is mandatory to enter a Work note to explain why the incident is being assigned to the new group or individual and what is expected of them.

Throughout this time the Work notes field is used to make journal style updates to the incident capturing what actions have been taken and what has been learnt. If an update needs to be provided to the original caller, this can be done using the Comments field.

When a fix is identified by the investigation, the assigned to individual will apply the fix to resolve the issue. This may be in the form of a workaround rather than a permanent solution. A change request is raised to apply the fix, and this is related to the incident in the Change Request field. If the incident is purely waiting for the change to be implemented and no other activities are occurring, the State field can be changed to On Hold with an On Hold reason of Awaiting Change.

Once the fix or workaround is applied, the Assigned To individual will test to see if the issue is resolved. If they believe it is, they will change the state field to Resolved or click the Resolve button.

## 6.11 Investigation and Diagnosis

Investigation and diagnosis is handled by Incident Support; this can be internal NOC team members or vendors and other third-party support and partners. The primary focus at this stage is to analyze and identify the cause of the incident, being sure to keep the incident record updated so that NOC Help Desk and users can be kept updated on the latest status.

| **ID** | **Activity** | **Description** |
| --- | --- | --- |
| INC 3.1 | Acknowledge Incident Assignment | Each 2nd level support group is responsible for monitoring their respective queues for assigned incidents   * Assign incident to specific support team member, Or * Reassign to another support group, if appropriate. |
| INC 3.2 | Investigate potential causes | Each support group involved with handling the incident investigates and diagnoses what has gone wrong. Key activities should include investigating potentially related records:   * Configuration Items * Changes * Problems/Known Errors * Once investigation is complete, the support groups attempt to diagnose the cause |
| INC 3.3 | Update Incident Record | In the Notes section:   * Update Additional Comments field with customer visible details on the status * Update Work notes field with details of all activities performed to this point * If a diagnosis was determined, go to INC 4.0 |
| INC 3.4 | Functional Escalation | * If a diagnosis was not determined by the current support group, the incident record can be reassigned to another support group for further assistance. Return to INC 3.1 * If a diagnosis was not determined within SLA/OLA/UC expected time, the SLA monitor escalates the priority of the incident, and leaves a marker as to its progress |

The incident is put into On Hold state by changing the State field. The On Hold reason field becomes mandatory at this point with the following choices:

* Awaiting Caller
* Awaiting Change
* Awaiting Problem
* Awaiting Vendor

Putting something on hold (Awaiting Caller) will typically act as the pause condition for all SLAs.

The mandatory fields in this state are:

* Problem when “Awaiting Problem” is set.
* Change when “Awaiting Change” is set
* Category
* Additional comments when “Awaiting Caller” is set.

## 6.12 Resolution and Recover

Resolution and Recovery is handled by Incident Support; this can be internal NOC team members or vendors and other third-party support and partners. The primary focus at this stage is to identify and implement the incident resolution. If the root cause of the incident was not identified or a permanent solution was not implemented, a problem record can be generated from the incident record for further analysis.

| **ID** | **Activity** | **Description** |
| --- | --- | --- |
| INC 4.1 | Identify Resolution | * Once the diagnosis is determined, the resolution to restore service is identified * If a change is needed to implement the resolution, initiate a new RFC from the incident record. Proceed to INC 4.2 once the change request has been approved |
| INC 4.2 | Implement Resolution | * Follow documented procedures to implement the resolution or workaround * If the resolution or workaround implemented did not resolve the incident, go to INC 3.2 * Incident record State is updated to “Resolved” |
| INC 4.3 | Update/Validate Data in Incident Record | * Ensure the initial incident categorization still corresponds to the nature of the incident. Adjust if necessary * Update Additional Comments field with customer visible details on resolution * Update Work notes field with details of all activities performed to this point * If a defined known error workaround was not used and root cause was not identified, or a permanent solution was not implemented, a problem record is opened from within the incident record |

In order to move the State to Resolved, the Assigned To individual will need to give some further details to explain what the problem was and how it was fixed. The mandatory fields are:

* Resolution code
* Resolution notes

The Resolution codes field is a choice list focused on the nature of the resolution provided. The current list of resolution codes is listed below.

* Solved (Work Around)
* Solved (Permanently)
* Solved Remotely (Work Around)
* Solved Remotely (Permanently)
* Not Solved (Not Reproducible)
* Not Solved (Too Costly)
* Closed/Resolved by Caller

Resolution notes is a free text field intended to describe what the issue was and how it was resolved. This is deliberately not held as a category or choice list solution.

The Caller has 7 days to verify the resolution. To reopen the incident, they can use the email notification sent when the incident was resolved. This will set the State field back to In Progress and clear the Resolution code and notes. The Assigned To individual will receive a notification containing the Additional comments from the Caller.

If the Caller agrees with the resolution, they do not need to take any action. The incident will remain as Resolved for 7 days. After that time the State field is automatically updated to Closed.

## 6.13 Incident Closure

Closure of Incident is handled by the NOC Help Desk or automated closure. The primary focus at this stage is to notify the user of the incident resolution, confirm the resolution (either one-on-one or, automatically, through non‐response to notification email) and set the state of the incident record to “Closed”.

| **ID** | **Activity** | **Description** |
| --- | --- | --- |
| INC 5.1 | Notify of Resolution | When an incident is set to a Resolved incident state, an email notification is sent to the caller |
| INC 5.2 | Confirm Incident Resolution | * If satisfied with the resolution, user may ignore the notification, as no additional action is required * If not satisfied with the resolution, user can reopen the incident by clicking on the link within the email notification   If the resolution is not accepted and incident is reopened:   * NOC Help Desk or the assignment group validates that this is the same occurrence of the incident * If it is, go to INC 3.0 * If it is a new occurrence, a new incident should be created for tracking purposes and for potential problem analysis |
| INC 5.3 | Close Incident | * ServiceNow automatically closes the incident after 7 calendar days if the caller has agreed with the resolution * If the Knowledge check box is selected, a knowledge article is generated in a “Draft” state with the information from the incident. This practice is useful for knowledge management and knowledge-centered support. It can reduce the number or length of repeat incidents by distributing the information related to the incident * Customer satisfaction surveys are generated when incidents are closed to gather information about the quality of service received by the caller |

## 6.14 RACI Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Activities** | **Caller** | **NOC Help Desk** | **Incident Manager** | **Assignment Groups (2nd and 3rd Level) Support** |
| **INC 1.0** | **Incident Identification and Classification** | | | | |
| INC 1.1 | Log new incident | R/C | R | A |  |
| INC 1.2 | Verify User information | R/C | R | A |  |
| INC 1.3 | Capture Incident Details | R/C | R | A |  |
| INC 1.4 | Categorize incident | C | R | A |  |
| INC 1.5 | Prioritize incident | C/I | R | A/I |  |
| **INC 2.0** | **Initial Support** | | | | |
| INC 2.1 | Perform incident matching |  | R | A |  |
| INC 2.2 | Associate incident to related record |  | R | A |  |
| INC 2.3 | Search Knowledge |  | R | A |  |
| INC 2.4 | Apply Documented Resolution |  | R | A |  |
| **INC 3.0** | **Investigation and Diagnosis** | | | | |
| INC 3.1 | Acknowledge incident assignment |  | I | A | R |
| INC 3.2 | Investigate and diagnose |  |  | A | R |
| INC 3.3 | Update incident record | I | I | A | R |
| INC 3.4 | Functional escalation | I | I | A | R/I |
| **INC 4.0** | **Resolution and Recovery** | | | | |
| INC 4.1 | Identify Resolution |  | I | A | R |
| INC 4.2 | Implement Resolution |  | I | A | R |
| INC 4.3 | Update/validate data in incident record | I | I | A | R/I |
| **INC 5.0** | **Incident Closure** | | | | |
| INC 5.1 | Notify of resolution | I | R | A |  |
| INC 5.2 | Confirm Incident resolution | C/R | I/R | A |  |
| INC 5.3 | Close Incident |  | I/R | A |  |
|  | R: Responsible A: Accountable C: Consulted I: Informed | | | | |

## 6.15 Major Incident Management

Major incidents are managed as a sub process occurring within Incident Management where the impact of the incident is considered to have a particularly strong impact on the business such that additional activities must be undertaken to ensure the impact is reduced or removed as quickly as possible.

Major incidents are coordinated by a single individual, a Major Incident Manager, who will manage the situation through to resolution. The Major Incident Manager can use incident tasks to allow multiple support groups and users to work on the resolution concurrently. Incident Managers use the Major Incident Workbench to communicate regular updates on the progress of the incident through the lifecycle. When the incident has been resolved, the Incident Manager can conduct a review of the incident and any follow up activities.

| **ID** | **Activity** | **Description** |
| --- | --- | --- |
| MIM 1.0 | Propose new Major Incident | * Incident manager and/or an agent can propose a major incident in ServiceNow when an incident meets the major incident criteria is met. * Initiate major incident escalation process |
| MIM 1.1b | Assign to Major Incident group and manager | * Major incident is assigned to the major incident management group * Escalation is sent to the appropriate group as determined |
| MIM 1.2 | Communications to Business stakeholders | * Establish major incident management conference bridge * Initial communications about the issue and known workaround if available to be sent to all business stakeholders |
| MIM 1.3 | Communications to Technical solvers | * Send communications via email/on-call notification to technical resolvers required * Major Incident Manager engages support team members from required functional areas to investigate the issue |
| MIM 1.4 | Create conference bridge\* to discuss investigation steps and assign task | P1 Incident/Outage Response   * Upon receiving a P1 incident/outage, the NOC personnel will establish a bridge and notify the NOC-M and the D2C2 Chief Engineer or their designates via phone, email, and text (found in Appendix A), in order to join the bridge. * The NOC will send a status email every 15 minutes for the first two hours and every half hour after that until issues are resolved to all persons identified in the NOC Procedure 7.1 Appendix A. * The D2C2 Chief Engineer will notify the D2C2 ISSO via phone, email and text to join the bridge. * The D2C2 ISSO will advise the D2C2 ISSM. The D2C2 ISSM will determine if the contingency plan is to be enacted. * Once D2C2 Contingency Plan is enacted:   + The D2C2 ISSM assumes the role of Contingency Plan Director (CPD)   + The D2C2 ISSO assumes the role of Contingency Plan Coordinator (CPC)   + The D2C2 Chief Project Engineer assumes the role of Outage and Damage Assessment Lead (ODAL)   + The NOC-M assumes or assigns the role of Procurement and Logistics Coordinator (PLC)   P2 Incident/outage Response   * Upon receiving a P2 incident/outage, the helpdesk will notify the P2 response team (found in appendix B) or their designates, in order to establish a conference bridge within 30 minutes.   A status email shall be sent every 30 minutes for the first four hours and every half hour after that |
| MIM 1.5 | Assign tasks to individuals or using on-call scheduling | * Assign tasks to appropriate individuals from right resolver groups as needed |
| MIM 1.6 | Investigate task | * Task for technical support team investigates the recovery options, solution and workaround |
| MIM 1.7 | Diagnose and fix task | * Support team to make a decision, if the solution/workaround or recovery options are available * Operations Management and Support team to make a decision if Business Continuity Plan or Disaster Recovery Plan should be invoked |
| MIM 1.8 | Provide Fix update to parent Incident | * Update resolution details/workaround details to update parent incident * Identify the need for Problem record to be created |
| MIM 1.90 | Incident resolved | * All tasks are completed, service restored with a permanent fix or workaround |
| MIM 1.91 | Conduct Post Incident Review | * Create Problem record to identify the root cause of the issue * Audit all the steps executed during MIM, identify process guide update needs if any |
| MIM 1.92 | Communicate post incident review | * Send out Incident Review summary report to all stakeholders on issue description, root cause, solution implemented etc. and close out MIM |

\* Business stakeholders and technical teams will use a single conference bridge during the Major Incident investigation and resolution.

## 6.16 Non-Technical Urgent Issues

| **ID** | **Activity** | **Description** |
| --- | --- | --- |
| NTUI 1.0 | Request identified as a Non-Technical, Urgent Issue | * Security related issues |
| NTUI 1.1 | Create incident ticket | * The NOC team will enter all of the necessary information pertaining to the security issue. * It will assign the ticket to the D2C2 Operations Team |
| NTUI 1.2 | Contact SOC | * NOC team member will contact the SOC team (1800- Deloitte) * Provide all of the necessary details related to the issue |
| NTUI 1.3 | Inform project stakeholders | * NOC team will contact and inform Project Stakeholders to include Security |
| NTUI  1.4 | Inform Customer Stakeholders | * Management to contact and inform Customer Stakeholders of the current security issue |
| NTUI  1.5 | Update Ticket | * NOC team to update the incident ticket as more information is known * They will provide all the necessary assistance in order to resolve the issue |
| NTUI  1.6 | Close Ticket | * Incident ticket will be closed once confirmation from the SOC team is had on the issue being resolved. |

## 6.17 Incident Candidates

Users of the incident process may consider an incident to require the major process; however, they cannot automatically promote an incident into this process since it will trigger a number of actions and activities in other teams that they may not be aware of. Incidents are initially proposed as a Major Incident Candidate so that Incident Managers can confirm this process should be followed. There are 3 possible ways to do this:

* **Automatically via predefined trigger criteria**: Major incident candidates can be automatically proposed based on pre-defined criteria. When this criterion is met the incident is immediately proposed as a candidate
* **Manually from an existing incident**: Users can manually propose a candidate from an existing incident by selecting the Propose Major Incident choice in the context menu.
* **Manually where no incident currently exists**: If an incident does not already exist, a candidate can be proposed directly from the left navigation menu using the Create Major Incident Candidate option
* **Manually creating a major incident**: Major Incident Managers can create a major incident without the need for a candidate by using the Create Major Incident link in the left navigation menu.

## 6.18 Incident Communication Plan

Incident Communication Plan is defined for major incidents which helps support the process, with conditions Priority is 1 or 2 and MI is accepted. The plan helps guide sending communications to:

* Internal/Business Stakeholders
* Technical Teams
* End users

The plan creates communication tasks for the Major Incident Manager with specified trigger duration to guide him/her to send the communications to stakeholders.

| **Comm Plan** | **Task** | **Type** | **Frequency** | **Duration** |
| --- | --- | --- | --- | --- |
| Technical | Initial Technical Communication | Initial | One Time | 15 Mins |
| Technical Status Update | Status Update | Recurring | 30 Mins |
| Technical Resolution Communication | Resolution | Onetime | When Resolved |
| Internal Stakeholder | Internal Stakeholder Communications | Initial | One Time | 30 Mins |
| Stakeholder Status Update | Status Update | Recurring | 60 Mins  (P1 and P2) |
| Crisis Management Communication | Ad hoc | Recurring | 60 Mins  (P1 only) |
| Stakeholder Resolution Communication | Resolution | Onetime | When Resolved |
| End User\* | Initial End User Communications | Initial | One Time |  |
| End User Status Update | Status Update | Recurring |  |
| End User Resolution Communication | Resolution | Onetime |  |

The Major Incident Manager can use the Workbench to see much of the information associated with the major incident.

## 6.19 Major Incident Reviews

Once the major incident has been resolved, the Incident Manager will review what happened. This usually involves understanding the root cause, using Problem Management and concluding whether any steps can be taken to avoid the situation reoccurring, as lessons learned. The review is conducted when the incident is in Resolved state. If the review is comprehensive, incident tasks can be created and assigned. Once the review is complete, the incident will be closed manually by the Incident Manager.

## 6.20 Relationship with Other Processes

| **Process** | **Relationship** | **Input** | **Output** |
| --- | --- | --- | --- |
| Configuration Management | The configuration management system underpins all incident management activities. It not only hosts the incident and other service management records but contains details of the infrastructure components supporting business applications | X |  |
| When CI records are identified as inaccurate, incident records are created and assigned to configuration management for correction |  | X |
| Problem Management | Problems can be initiated from an incident when determining the root cause of the incident needs further investigation |  | X |
| Incident information is proactively analyzed to detect trends in service behavior that may be indicative of an underlying problem |  | X |
| Information about known errors and their workarounds is used to diagnose and resolve recurring incidents faster | X |  |
| Change Management | A request for change (RFC) can be submitted to implement a workaround or a resolution |  | X |
| Can detect and resolve incidents that arise from changes | X |  |
| Change management is responsible for keeping the Service Desk informed of all scheduled changes | X |  |
| Service Level Management | Defines measurable responses to service disruptions |  | X |
| Provides historical data that enables SLM to review service level agreements (SLAs) objectively and regularly |  | X |
| Assists SLM in defining where services are at their weakest so that SLM can define actions as part of the service improvement plan (SIP). |  | X |

Table 2: Incident Management Process Flow Chart



# Change Control Process

## 7.1 Principles and Basic Concepts

This process will provide a detailed explanation on how the Change Management process is enabled within the ServiceNow platform.

Change Management (“CM”) is a process that ensures that IT efficiently and effectively responds to and manages change at a pace and risk level consistent with the goals and objectives of the organization.

A Service Change is a change to an existing service or the introduction of a new service that results in an addition, modification or removal of authorized, planned or supported service(s) or component(s) that is formally approved by the appointed Change authority.

Changes should be cost effective and enhance business processes with minimum risk to the IT infrastructure and business operations.

Changes are made for a variety of reasons, for example:

* Proactively, when the business seeks benefits such as reduction in costs, improved services or increased ease and effectiveness of support.
* Reactively, as a means of resolving errors and adapting to changing circumstances.

## 7.2 Process Description

A change is the addition, modification or removal of anything that could have an effect on an IT service. Change Management is the process responsible for controlling the life cycle of all changes to minimize the risk of disruption to IT services.

Change Management relies heavily on:

* The Configuration Management process for change risk and impact analysis.
* The Release Management process for the building, testing and deployment of changes.

## 7.3 Process Goal and Objectives

The goal of the Change Management process is to enable beneficial changes to be made with minimum disruption to business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Change Management should apply a consistent approach to risk assessment, business continuity, change impact, resource requirements and change approval. The approach should maintain a proper balance between the need for a change and the timing of its integration into the live environment.

The objectives of Change Management are to:

* Respond to the customer’s changing business requirements while maximizing value and reducing incidents, disruption and rework.
* Respond to the business and IT requests for change that will align the services with the business needs.
* Ensure the changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner.
* Ensure that all changes to configuration items (CIs) are recorded in the Configuration Management Database (CMDB) (housed in SNOW).

## 7.4 Policies

The following policy statements were developed as part of the Plan and Analyze phase for the Change Management process. Compliance to all policy statements will be governed and enforced. Exceptions must be identified and approved through the governance board.

* All changes to the IT environment must follow the formal Change Management process.
* All changes must be documented in the accepted Change System of Record (SOR) – ServiceNow.
* All changes must identify Change Type, which is predefined and agreed upon by all stakeholders.
* All changes must include a back-out procedure unless explicitly decided and approved by CAB when back-out is unnecessary or not possible.
* All changes must include a valid Implementation Plan, which must be followed to implement the change.
* All changes must have a validation plan to confirm or deny the expected results of the changes post implementation.
* All change requests must receive a formal approval prior to change implementation.
* Emergency change can only be used to resolve a critical or major incident.
* Change Initiator will be held accountable to confirm the accuracy and completeness of the change request.
* Change Reviewers will be held accountable for a complete review of the change.
* Change Owner is accountable for the coordination and completion of the change.
* All changes must be technically verified, and user accepted (where possible).
* All changes must be formally closed post implementation within a stipulated period of time.
* All services must have a defined Change Maintenance Window.
* Changes must follow the established Lead Times based on Change Priority.

## 7.5 Process Scope

The scope of Problem Management includes:

* Changes from IT users for maintaining IT infrastructure that would need change or replacement of hardware or software.
* Changes from IT users that involve resolution or recovery of an IT service(s) that has an open incident and will require a change or replacement of hardware or software.
* Changes to IT services, processes, hardware, or software considered in production and/or CIs that are managed in CMDB.
* Change Management process will include all subprocesses and activities defined by ITIL Change Management process.

## 7.6 Methods of Raising an RFC

There are several ways to generate a new change record in ServiceNow:

* Create a change manually through the Change application.
* Copy an existing change.
* Request a change through the Service Catalog.
* Initiate a change from an incident.
* Initiate a change from a problem.
* Initiate from a CI or list of CI’s.

## 7.7 Change Types

To streamline the Change Management process, change types are established to categorize a change request so that there is a clear process for each change type. Change types drive enforcement of lead time, approvals workflows or whether or not a change requires a CAB review. There are three (3) types of changes:

1. **Standard Changes** are types of changes that have had their associated Change Proposals approved by Change Management and CAB.
2. **Normal Changes** are types of changes that follow a normal change process flow and will require one of multiple review(s) and approval(s) for implementation.
3. **Emergency Changes** are associated strictly to resolve a P1 or P2 incident or prevent an imminent failure.
4. **Configuration change** requests are classified as needed changes to IT components or assets.
5. **Rollback Change** requests occur when the actions of an associated change request need to be reversed. Rollback changes will need to go through the CAB.
6. **User Creation** requests allow for new accounts to be created. This request has its own approval process and does not go through the CAB.
7. **User Termination** requests are submitted when accounts need to be terminated or disabled. This occurs when users are noncompliant with security policies or have either left or been transferred.
8. **Updates and Patches** may be requested in order to implement a new software release, or apply a fix to repair any issues within the system
9. **Software Install** requests will go through the change control process whenever a client requests certain software installation.

## 7.8. Standard Changes

Standard Changes are types of changes that have had their associated Change Proposals approved by Change Management and CAB. These changes have been assessed as being low risk and have a repeatable implementation plan. Standard changes can only be raised by selecting from an existing template available in the Standard Change Catalog. This catalog provides a means for the Change Management team to control which changes can be raised through the Standard Change process. This catalog contains a list of templated changes that have been approved as Standard changes. For a change to qualify as a “Standard”, the change must have the following conditions:

|  |  |
| --- | --- |
| **Condition** | **Standard** |
| **Lead Time for Implementation** | None |
| **Risk Level** | 5-Low |
| **Business Executive Approval** | N/A |
| **Change Management Approval** | Pre-Approved |
| **Technical Approval** | N/A |
| **Support Team Approval** | N/A |
| **Business Approval** | N/A |
| **CAB Review** | Pre-Approved |

## 7.9 Normal Changes

Normal Changes are types of changes that follow a normal change process flow and will require one of multiple review(s) and approval(s) for implementation. As a best practice, we define three sub-types of Normal changes:

## 7.9.1 Normal Minor

A Normal Minor change is a type of change that is evaluated against a number of factors such as affecting a non-critical configuration item, having a low impact to the business and having a risk score that meets the conditions for ServiceNow to assess the change as minor. Normal Minor changes have the following conditions.

|  |  |
| --- | --- |
| **Condition** | **Normal Minor** |
| **Lead Time for Implementation** | 24 hrs. |
| **Risk Level** | 5- Low |
| **Business Executive Approval** | No |
| **Change Management Approval** | Yes |
| **Technical Approval** | Yes |
| **Support Team Approval** | Yes |
| **Business Approval** | No |
| **CAB Review** | N/A |

## 7.9.2 Normal Significant

A Normal Significant change is a type of change that is evaluated against a number of factors such as affecting a critical configuration item, having a high impact to the business and having a risk score that meets the conditions for ServiceNow to assess the change as Significant. Normal Significant changes have the following conditions.

|  |  |
| --- | --- |
| **Condition** | **Normal Significant** |
| **Lead Time for Implementation** | 7 Calendar Days |
| **Risk Level** | 4-Moderate to 1-Critical |
| **Business Executive Approval** | No |
| **Change Management Approval** | Yes |
| **Technical Approval** | Yes |
| **Support Team Approval** | Yes |
| **Business Approval** | Yes |
| **CAB Review** | Local or Enterprise |

## 7.9.3 Normal Expedited

A Normal Expedited change is a type of change that does not meet the required lead time for implementation. These are changes that are not associated with a P1 or P2 incident to restore service, rather these are changes that cannot have a minimum lead time of 7 days. Normal Expedited changes have the following conditions.

|  |  |
| --- | --- |
| **Condition** | **Normal Expedited** |
| **Lead Time for Implementation** | None |
| **Risk Level** | 5-Low to 1-Critical |
| **Business Executive Approval** | Yes |
| **Change Management Approval** | Yes |
| **Technical Approval** | Yes |
| **Support Team Approval** | Yes |
| **Business Approval** | Yes |
| **CAB Review** | Expedited (virtual) |

## 7.10 Emergency Change

Emergency Changes are associated strictly to resolve a P1 or P2 incident or prevent an imminent failure. To log an Emergency Change, a Change Requester must create a change request directly from a P1 or P2 incident record. Emergency Changes are verbally approved by ECAB, and documentation of the change request occurs after implementation.

|  |  |
| --- | --- |
| **Condition** | **Emergency** |
| **Lead Time for Implementation** | None |
| **Risk Level** | 5-Low to 1-Critical |
| **Business Executive Approval** | Verbal |
| **Change Management Approval** | No |
| **Technical Approval** | No |
| **Support Team Approval** | No |
| **Business Approval** | No |
| **CAB Review** | Emergency CAB |

## 7.11 Change State (ServiceNow)

States in any ServiceNow application serve a specific purpose. They are designed to make it clear where in a process a particular record currently resides and to display progress. Change Management has the following states:

| **ServiceNow Problem state** | **Description** | **Change Process Area** |
| --- | --- | --- |
| New | Default value upon creation. |  |
| Assess | Assess quality of change information and risk and impact of change. |  |
| Authorize | Approve change. |  |
| Scheduled | Change is approved, awaiting implementation. |  |
| Implement | Change is being implemented. |  |
| Review | Review results of implemented change. |  |
| Closed | Change is complete. |  |
| Canceled | Change has been cancelled. |  |

All change requests must receive a formal approval prior to change implementation. Depending on the type of change, the approval workflow may be slightly different for each type.

## 7.12 Change Collision

A collision occurs when a CI is related to two or more change requests whose implementation schedules overlap. ServiceNow Change Management helps us manage change collisions between change requests and helps us make decisions to manage and resolve the potentially harmful conflicts between these change requests. Listed below are a few scenarios of change collision:

* Conflicting change with the same Affected CI’s.
* Change occurring during blackout window.
* Change occurring outside CI Maintenance Schedule.
* Changes with the same “assigned to” person.

## 7.13 Change Calendar

The Change Conflict Calendar (as per ServiceNow) graphically represents the changes, blackout and maintenance window related to a change request and helps to visually display potential conflicts.

The Change Conflict Calendar supports configuration to control the display of related changes that are scheduled for the same date and time depending on the value of the Assigned tTo, Assignment Group or Configuration item field.

The Change Conflict Calendar, by default, displays the schedule of the change for the planned start day. To view details of a specific day, you can click the Calendar (view-calendar-icon) icon at the upper left of the window and select a date. You can click Today to view the change schedule of the current day or month. The left and the right arrow next to Today (view-calendar-today) helps you to navigate to the previous or the next day or month depending on the view type.

Conflict detection uses blackout and maintenance schedules to find potential scheduling conflicts for the configuration items associated with a change request. When conflict detection runs, either automatically or by manual request, conflict detection determines if either type of defined schedule applies to the change request. If a potential conflict is identified, a warning message appears, and conflicts are listed within the Conflict form section.

## 7.14 Blackout Window

Blackout windows specify times during which normal change activity should not be scheduled. Maintenance windows specify times during which change requests should be scheduled. For example, create a blackout schedule for code freezes at the end of the year.

## 7.15 Maintenance Window

A maintenance window is a defined period of time during which planned outages and changes to production services and systems may occur. The purpose of defining maintenance windows is to allow business to prepare for possible disruption of service. Standard maintenance windows are associated to the CIs in the CMDB and can be visible from the Change Calendar.

## 7.16 Change Assessment and Evaluation

The potential impact on the services of failed changes and their impact on service assets and configurations need to be considered. The following questions must be answered for all changes. Without proper information, the impact assessment cannot be completed, and the balance of risk and benefit to the live service will not be understood. This could result in the change not delivering all the possible or expected business benefits or even having a detrimental, unexpected effect on the live service.

1. Who RAISED the change?
2. What is the REASON for the change?
3. What is the RETURN required from the change?
4. What are the RISKS involved in the change?
5. What RESOURCES are required to deliver the change?
6. Who is RESPONSIBLE for the build, test and implementation of the change?
7. What is the RELATIONSHIP between this change and other changes?

## 7.28 Change Impact Analysis

Change Impact Analysis involves understanding the impact of the change to other CIs that are dependent on or related to the CI which is being changed. Change Impact Analysis can effectively be done using an up to date CMDB and tools that provide a graphical view of the CI relationship.

## 7.29 Change Risk Assessment

Risk assessment is defined as Analyzing the value of service assets to the business, identifying threats to those assets due to the proposed change and evaluating how vulnerable each service asset is to those threats. Risk Assessment can be quantitative (based on numerical data) or qualitative.

## 7.30 Change Process Roles and Responsibilities

The following table describes the typical roles defined for Problem Management process.

| **Process Role** | **Responsible for** | **ServiceNow (System) Role** |
| --- | --- | --- |
| Change Process Owner | * Accountable for process development, maintenance, improvement, execution and outcomes at an agreed performance. * Develops and is ultimately responsible for the process design, documents and communicates the process. * Works with Process Governance to define KPIs to evaluate the process effectiveness and efficiency, risk profile and control effectiveness of the process. * Reviews and analyzes KPIs and prioritizes improvement opportunities. * Implements and reviews improvement actions. * Addresses any issues with running the process. * Ensures all relevant staff have the required training in the process and are aware of their role in the process. * Ensures that the process, roles, responsibilities and documentation are regularly reviewed and audited. * Has the authority and ability to make changes in the process as required and approved by Service Management process governance. * Identifies standard changes across all domains, consolidates and makes it available in a single list. * Setting the scope and policies for Change Management process. |  |
| Change Manager(s) | * Responsible for successful execution of the Change Management process. * Planning and managing support for Change Management tools and processes. * Coordinating interfaces between Change Management and other ITSM processes. * Documenting and managing work instructions. * Monitor, track and control the Change Management process to meet the required service level targets. * Verifying that RFCs are correctly completed. * Assigns a Change Owner to all Request for Changes. * Responsible for identifying, creating, and maintaining Standard Changes. * Identify sensitive change periods and control the change throughout by Service Change. * Change Manager should attend CAB meetings as defined by the CAB charter. | Change manager |
| Change Owner/ Coordinator | * Submitting requests for evaluation to trigger the Change Evaluation process. * Formally communicating decisions of change authorities to affected parties. * Monitoring and reviewing activities of teams and functions that build and test changes to ensure that the work is carried out correctly. (This will also be carried out as part of the Release and Deployment Management process for a change that is part of a release.) * Change Owner should attend CAB meetings as defined by the CAB charter. * Accountable for the Change throughout its life cycle including back-out. |  |
| Change Initiator | * Identifying the requirement for a change. * Completing and submitting a change proposal if appropriate. * Completing and submitting an RFC. * Attending CAB meetings to provide further information about the RFC or change proposal if required. * Reviewing the change when requested by Change Management, and specifically before closure. * If Change Initiator and Requestor is not the same person, then the Change Initiator should confirm acceptance from the Change Requestor to complete the change cycle. |  |
| Change Implementer | * Reviewing tasks and its associated schedule to ensure that these tasks can be supported. * Release, Build and Deployment practitioner that implements the change. * Develops and updates the RFC with the Implementation and back-out Plans. * Updates the change record with task status and the actions taken. * Attending CAB meetings to discuss and review changes when required. |  |
| CAB/ECAB Member | * Participating in CAB/ECAB meetings to support the authorization of changes and to assist Change Management in the assessment and prioritization of changes. * Authority to represent a particular group or function. * Preparing for CAB/ECAB meetings by circulating RFCs within their own group and coordinating feedback. * Reviewing RFCs and recommending whether they should be authorized. * Reviewing successful and failed changes. * Reviewing unauthorized changes. * Reviewing the change schedule and providing information to help identify conflicts or resource issues. * Reviewing the projected service outage and providing feedback on the impact of planned outages. | Change approver |
| CAB/ECAB Chair | * Deciding who should attend CAB/ECAB meetings. * Planning, scheduling, managing and chairing CAB/ECAB meetings. * Selecting RFCs for review at CAB/ECAB meetings, based on the change policy. * Circulating RFCs in advance of CAB/ECAB meetings to allow prior consideration. * Convening Emergency Change Advisory Board (ECAB) meetings for consideration of Emergency changes. * Selecting successful and failed changes for review at CAB meetings. |  |

## 7.31 RACI Matrix

Roles and responsibilities are assigned to specific process activities.

| **ID** | **Activities** | **Change Manager** | **Change Requestor** | **Change Implementer** | **Approver** | **CAB Member** | **End User** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CHG 1.0** | **Normal Change** |  |  |  |  |  |  |
| CHG NC.5 | Create New RFC |  | A/R |  |  |  |  |
| CHG NC.1 | Document Change Details |  | A/R |  |  |  |  |
| CHG NC.15 | Document Change Plans |  | A/R |  |  |  |  |
| CHG NC.2 | Document Change Schedule |  | A/R |  |  |  |  |
| CHG NC.25 | Check Conflicts |  | A/R |  |  |  |  |
| CHG NC.3 | Submit for Approval | I | A/R | I |  |  |  |
| CHG NC.35 | Review Content | A/R | C | C |  |  |  |
| CHG NC.4 | Assess Risk | A/R | C | C |  |  |  |
| CHG NC.45 | Conduct Technical Assessment | I | C/I | C/I | A/R |  |  |
| CHG NC.5 | Authorize Change | A/R | I | I | R |  |  |
| CHG NC.55 | Prepare for Change Implementation | A/R |  | R |  |  |  |
| CHG NC.6 | Validate Change | I | I | A/R |  |  |  |
| CHG NC.65 | Conduct Post Implementation Review | A/R | C | C |  |  |  |
| **CHG 2.0** | **Emergency Change** |  |  |  |  |  |  |
| CHG EC.5 | Create New RFC |  | A/R |  |  |  |  |
| CHG EC.5 | Document Change Details |  | A/R |  |  |  |  |
| CHG EC.5 | Document Change Plans |  | A/R |  |  |  |  |
| CHG EC.5 | Document Change Schedule |  | A/R |  |  |  |  |
| CHG EC.5 | Check Conflicts |  | A/R |  |  |  |  |
| CHG EC.5 | Submit for Approval | I | A/R | I |  |  |  |
| CHG EC.5 | Review Content | A/R | C | C |  |  |  |
| CHG EC.5 | Assess Emergency Change | A/R | C | C |  | R |  |
| CHG EC.5 | Prepare for Change Implementation | A/R |  | R |  |  |  |
| CHG EC.5 | Validate Change | I | I | A/R |  |  |  |
| CHG EC.5 | Conduct Post Implementation Review | A/R | C | C |  |  |  |
| **CHG 3.0** | **Standard Change Template** |  |  |  |  |  |  |
| CHG ST.5 | Access Template Manager |  | A/R |  |  |  |  |
| CHG ST.1 | Request a New Template | I | A/R |  |  |  |  |
| CHG ST.15 | Request to Modify a Template | I | A/R |  |  |  |  |
| CHG ST.2 | Request to Retire a Template | I | A/R |  |  |  |  |
| CHG ST.25 | Review and Approve Proposal | A/R | C | C |  | C |  |
| **CHG 4.0** | **Standard Change** |  |  |  |  |  |  |
| CHG SC.5 | Select Service |  |  |  |  |  | A/R |
| CHG SC.1 | Obtain Approvals |  | I |  |  |  | A/R |
| CHG SC.15 | Create New RFC |  | A/R |  |  |  |  |
| CHG SC.2 | Document Change Details |  | A/R |  |  |  |  |
| CHG SC.25 | Document Change Plans |  | A/R |  |  |  |  |
| CHG SC.3 | Document Change Schedule |  | A/R |  |  |  |  |
| CHG SC.35 | Check Conflicts |  | A/R |  |  |  |  |
| CHG SC.4 | Submit Standard Change | I | A/R | I |  |  |  |
| CHG SC.45 | Prepare for Change Implementation | A/R |  | R |  |  |  |
| CHG SC.5 | Validate Change | I | I | A/R |  |  |  |
| CHG SC.55 | Conduct Post Implementation Review | A/R |  |  |  |  |  |
| R: Responsible A: Accountable C: Consulted I: Informed | | | | | | | |

## 7.32 Change Management Process Activities

The Change Management process is designed to manage the Change lifecycle including: submission, assessment, authorization, implementation and review & closure.

| ID | Activity | Description |
| --- | --- | --- |
| CHG 1.0 | Change Submission | This process activity involves creating change request in ServiceNow via the RFC. The Requester is expected to provide most if not all the information required for the submission of the RFC. The risk assessment is also completed during this phase. |
| CHG 2.0 | Change Assessment | This process activity involves Change Management to assess and validate the required artifacts and that the overall request meets the MOR and is compliant with all change processes and policies. |
| CHG 3.0 | Authorization | This process activity involves seeking approvals. All approval entities are sent an email that is generated by ServiceNow that is dependent on the type of change. A change request moves to the next stage of the lifecycle if all approvals are obtained. |
| CHG 4.0 | Implementation | This process activity involves change implementers completing change tasks that are assigned that includes:   1. Testing Task: This task is required for testing activities. 2. System Review: This task is required to ensure that there are no new ports, services, or anything else configured on the system before it is put into production. This will be accomplished through our Tennable System Scans. 3. Implementation Task(s): This task, along with any other customer implementation tasks created by the change request, is to track the actual implementation task. The Planned Start/End Date must not be outside of the RFC change window. 4. An Update CMDB Task: This task is required if there is a need to update the CMDB with updates as impacted by the change. ServiceNow is configured to only allow assigning this task to an individual who holds the credentials to update the CMDB. If this task is not required, the task can be cancelled. 5. A Post Implementation Review Task: This task is only required to be fulfilled if a change request was unsuccessful or was implemented unsuccessfully with issues. If this task is not required, the task can be cancelled. |
| CHG 5.0 | Review & Closure | This process activity involves validating that the implementation was successful and conducting a post implementation review for changes that were unsuccessful or unsuccessful with issues. |

A Normal change is one that follows the full lifecycle and typically does not fall into any of the other types. There may still be differences in the activities that occur for a normal change. For example, a normal significant change would likely have more approval layers attached to it than a low risk one. Normal changes typically have lead times associated with them to allow the relevant Change Managers, approvers and CAB the appropriate amount of time to review them and feel comfortable before proceeding.

## 7.33 Normal Change: Planning and Submission

| ID | Activity | Description |
| --- | --- | --- |
| **Planning & Submission** | | |
| NCHG 1.1 | Draft New Change Request | Under the Change category in ServiceNow, select “Create New” and then select “Normal” as the change type. |
| NCHG 1.2 | Define Business Justification | Justify the reason for the change in the planning tab of the RFC. |
| NCHG 1.3 | Complete High-Level Plan (Implementation plan, backout plan, etc.) | Provide all required information for the high-level plans in the planning tab of the RFC. |
| NCHG 1.4 | Identify Affected CI(s) | Select all CIs that will be affected by the change request. |
| NCHG 1.5 | Select Target Change Implementation Window | Select a start and end date and time to implement standard change and have all the necessary tasks within the same timeframe. |
| NCHG 1.6 | Check for Conflicts | Ensure there are no conflicts identified in the Change Record, otherwise have all conflicts identified resolved. |
| NCHG 1.7 | Identify Implementation Build Team | Assign the change to the appropriate implementation team. |
| NCHG 1.8 | Conduct Risk Assessment | Complete all questions in the risk assessment to allow ServiceNow to categorize the risk level. |
| NCHG 1.9 | Set Normal Change Type to Minor | ServiceNow categorization of risk that is dependent on the selected CI, planned start date and risk assessment. |
| NCHG 1.10 | Set Normal Change Type to Significant | ServiceNow categorization of risk that is dependent on the selected CI, planned start date and risk assessment. |
| NCHG 1.11 | Set Normal Change Type to Expedited | ServiceNow categorization of risk that is dependent on the selected CI, planned start date and risk assessment. |
| NCHG 1.12 | Provide Expedited Reason | For Normal Change Requests that are categorized as “Expedited”, must provide a justification to why it needs to be. |
| NCHG 1.13 | Submit Change for Assessment | Submit the RFC for Change Management to assess and provide feedback. |

## 7.34 Normal Change: Assessment

| ID | Activity | Description |
| --- | --- | --- |
| **Assessment** | | |
| NCHG 2.1 | Validate Business Justification and Criticality | Project Chief Engineer and NOC-M to validate if expedited change request is business critical. |
| NCHG 2.2 | Verify RFC Details (Type of Change, Risk, impact, conflicts, scheduling) | Change Management to confirm the RFC is of the correct change type, the risks associated to the change, and that there are no conflicts. |
| NCHG 2.3 | Provide PAC/OAC/MOR Guidelines | Change Management to determine and provide list of artifacts from the PAC/OAC and MOR guidelines for Change Requester to complete. |
| NCHG 2.4 | Select Target CAB Date | Change Management to select the type of CAB required to review and approve/reject the change request, as well the date to present the change in CAB. |
| NCHG 2.5 | Validate Testing and Close Testing Task | Conduct all testing and close the testing task before submitting the Change Request for approvals. |
| NCHG 2.6 | Coordinate Design, Build, Test Activities, Confirm Implementation Plan and Resources | Requester to plan the design, build and test activities with the implementation groups and propose any CI changes as necessary. |
| NCHG 2.7 | Complete All PAC/OAC/MOR Requirements | Complete all required artifacts from the PAC/OAC list provided by Change Management. |
| NCHG 2.8 | Submit Change for Approval | Submit completed RFC for approval. |

## 7.35 Normal Change: Authorization and Scheduling

| ID | Activity | Description |
| --- | --- | --- |
| **Authorization and Scheduling** | | |
| NCHG 3.1 | Review and Approve PAC Requirements, Validate Risk and Implementation Plan, and Proposed CI Changes | Technical approver to review the artifacts from the PAC and proposed CI changes, as well validate the risk and implementation plan. |
| NCHG 3.2 | Review and Approve Transition and OAC Requirements | Support Team approver to review and approve the artifacts from the OAC and validate transition. |
| NCHG 3.3 | Review and Approve Business Impacts and PAC Requirements | Business approver to validate and approve change based on business impacts |
| NCHG 3.4 | Review Change in CAB Meeting | The RFC is presented and discussed in the CAB. The CAB will either approve/reject the RFC. |

## 7.36 Normal Change: Implementation

| ID | Activity | Description |
| --- | --- | --- |
| **Implementation** | | |
| NCHG 4.1 | Indicate Start of Implementation | Implementation team must indicate when they are starting a task in ServiceNow. |
| NCHG 4.2 | Perform Deployment Tasks as Per Implementation Plan | Change tasks in the implementation plan are completed by the implementation team. A system review will be completed in order to verify that no new ports, services, or anything else is configured on the system. To be completed using the Tennable System Scans. |
| NCHG 4.3 | Validate Implementation Results | Once a task is performed, the implementation team will verify the task has been completed successfully. |
| NCHG 4.4 | Initiate Backout Plan | If any change tasks performed created a disruption to the business service or application, the specified rollback plan will be initiated. |
| NCHG 4.5 | Update CMDB | If necessary, the CMDB will be updated to reflect the changes made to one/multiple affected Configuration Items. |
| NCHG 4.6 | Document Implementation Results | The state of the task and implementation notes will be updated by the implementation team. Once all the tasks have been marked as complete, the change request will go into “Review” state. |

## 7.37 Normal Change: Review and Closure

| ID | Activity | Description |
| --- | --- | --- |
| **Review and Closure** | | |
| NCHG 5.1 | Review Change Outcome | Change management will review and validate the Normal change in “Review” state. This is to ensure the change has been implemented successfully. |
| NCHG 5.2 | Conduct Post Implementation Review | If the Normal change has been completed as “Successful with issues” or “Unsuccessful”, a Post-Implementation Review will be conducted to investigate the handling process of the change through the entirety of its life cycle, and reasons for failure. This documents the opportunities to improve similar future implementations. |
| NCHG 5.3 | Notify Stakeholders on PIR Report | Report of the investigation and findings will be documented and sent to the affected/impacted stakeholders of the change request. |
| NCHG 5.4 | Close RFC | If the Normal change has been completed as “Successful”, the Change management team will close the change request, or it will automatically close after 7 days as per Change Process Guidelines. |

## 7.38 Emergency Change

Emergency changes are initiated from an incident record. They introduce unanticipated risk into the environment by circumventing the majority of the Change Management process. As such, they should only be used for critical or high priority incidents that are causing impact or imminently will.

## 7.38.1 Emergency Change: Planning and Submission

| ID | Activity | Description |
| --- | --- | --- |
| **Planning and Submission** | | |
| ECHG 1.1 | Draft Emergency Change from a P1 or P2 Incident | Create an Emergency Change record via right-click option in ServiceNow on a Major Incident or a Priority 1 or 2 incident record. |
| ECHG 1.2 | Convene Emergency CAB | Verbal or email approval from a business executive is required in order to perform the Emergency Change. |

## 7.38.2 Emergency Change: Authorization and Scheduling

| ID | Activity | Description |
| --- | --- | --- |
| **Authorization and Scheduling** | | |
| ECHG 2.1 | Review Emergency Change | The RFC is presented and discussed in the Emergency CAB. The Emergency CAB will either approve/reject the RFC.  Committee consists of Chief Engineer, duty NOC manager, QA Lead, Customer Designate (for customer impacting changes) |
| ECHG 4.3 | Notify Stakeholders | Report of the investigation and findings will be documented and sent to the affected/impacted stakeholders of the change request. |
| ECHG 4.4 | Close RFC | If the Emergency change has been completed as “Successful”, the change request will automatically close immediately. |

## 7.38.3 Emergency Change: Implementation

| ID | Activity | Description |
| --- | --- | --- |
| **Implementation** | | |
| ECHG 3.1 | Indicate Start of Implementation | Implementation team must indicate when the task started in ServiceNow. |
| ECHG 3.2 | Perform Deployment Tasks As Per Implementation Plan | Change tasks are completed by the implementation team. A system review will be completed in order to verify that no new ports, services, or anything else is configured on the system. To be completed using the Tennable System Scans. |
| ECHG 3.3 | Validate Implementation Results | Once a task is performed, the implementation team will verify the task has been completed successfully. |
| ECHG 3.4 | Initiate Backout Plan | If any change tasks performed created a disruption to the business service or application, the specified rollback plan will be initiated. |
| ECHG 3.5 | Update CMDB | If necessary, the CMDB will be updated to reflect the changes made to one/multiple affected configuration items. |
| ECHG 3.6 | Complete Emergency Change Details | The Emergency Change record is completed in full, documenting all tasks completed, and overall change details. |

## 7.38.4 Emergency Change: Review and Closure

| ID | Activity | Description |
| --- | --- | --- |
| **Review and Closure** | | |
| ECHG 4.1 | Review Change Outcome | Change Management will review and validate the Emergency change in “Review” state. This is to ensure the change has been implemented successfully. |
| ECHG 4.2 | Conduct Post Implementation Review | If the Emergency change has been completed as “Successful with issues” or “Unsuccessful”, a Post-Implementation Review will be conducted to investigate the handling process of the change through the entirety of its life cycle, and reasons for failure. This documents the opportunities to improve similar future implementations. |
| ECHG 4.3 | Notify Stakeholders on PIR Report | Report of the investigation and findings will be documented and sent to the affected/impacted stakeholders of the change request. |
| ECHG 4.4 | Close RFC | If the Emergency change has been completed as “Successful”, the change request will automatically close immediately. |

## 7.39 Standard Change

Standard changes are often known as routine changes. This is a change that is frequently implemented, is considered low risk with repeatable implementation steps and has a proven history of success. Standard changes are pre‐approved by the Change Advisory Board (CAB) so that they can be raised and implemented as quickly as possible.

## 7.39.1 Standard Change: Planning and Submission

| ID | Activity | Description |
| --- | --- | --- |
| **Planning & Submission** | | | |
| STCHG 1.1 | Identify Standard Change via Standard Change Catalog | Identify whether the Standard Change template already exists in the Catalog. |
| STCHG 1.2 | Select Standard Change Template | Select from a list of pre-approved list of standard changes in the Standard Change Template Library. The list will be categorized based on the specificity of the change. |
| STCHG 1.3 | Complete Standard Change Form Details | Provide all necessary details into the Standard Change RFC in order for the implementation team to successfully implement change. |
| STCHG 1.4 | Submit Change for Implementation | Submit the standard change request to be implemented by the implementation team at the designated implementation start date. The requester is responsible to ensure that all the information in the change request is correct, and all necessary change tasks have been created. |

## 7.39.2 Standard Change: Implementation

| ID | Activity | Description |
| --- | --- | --- |
| **Implementation** | | | |
| STCHG 3.1 | Indicate Start of Implementation | Implementation team must indicate when they are starting a task in ServiceNow. |
| STCHG 3.2 | Perform Deployment Tasks as Per Implementation Plan | Change tasks in the implementation plan are initiated and completed by the implementation team. |
| STCHG 3.3 | Validate Implementation Results | Once a task is performed, the implementation team will verify the task has been completed successfully. |
| STCHG 3.4 | Initiate Backout Plan | If any change tasks performed created a disruption to the business service or application, the specified rollback plan will be initiated. |
| STCHG 3.5 | Update CMDB | If necessary, the CMDB will be updated to reflect the changes made to one/multiple affected Configuration Items. |
| STCHG 3.6 | Document Implementation Results | The state of the task and implementation notes will be updated by the implementation team. Once all the tasks have been marked as complete, the change request will go into “Review” state. |

## 7.39.3 Standard Change: Review and Closure

| ID | Activity | Description |
| --- | --- | --- |
| **Review and Closure** | | |
| STCHG 4.1 | Review Change Outcome | Change requester will review and validate the Standard change in “Review” state. This is to ensure the change has been implemented successfully. |
| STCHG 4.2 | Conduct Post Implementation Review (For Unsuccessful Changes) | If a Standard change has been completed as “Successful with issues” or “Unsuccessful”, a Post-Implementation Review will be conducted by Change Management to investigate the handling process of the change through the entirety of its life cycle, and reasons for failure. This documents the opportunities to improve similar future implementations. |
| STCHG 4.3 | Notify Stakeholders on PIR Report | Report of the investigation and findings will be documented and sent to the affected/impacted stakeholders of the change request. |
| STCHG 4.4 | Close RFC | If a Standard change has been completed as “Successful”, the change request will automatically close immediately. |

Table 3: Change Request Flow Chart



Table 4: GCP Create Account Sub-Process



Table 5: Updates and Patches Sub-Process

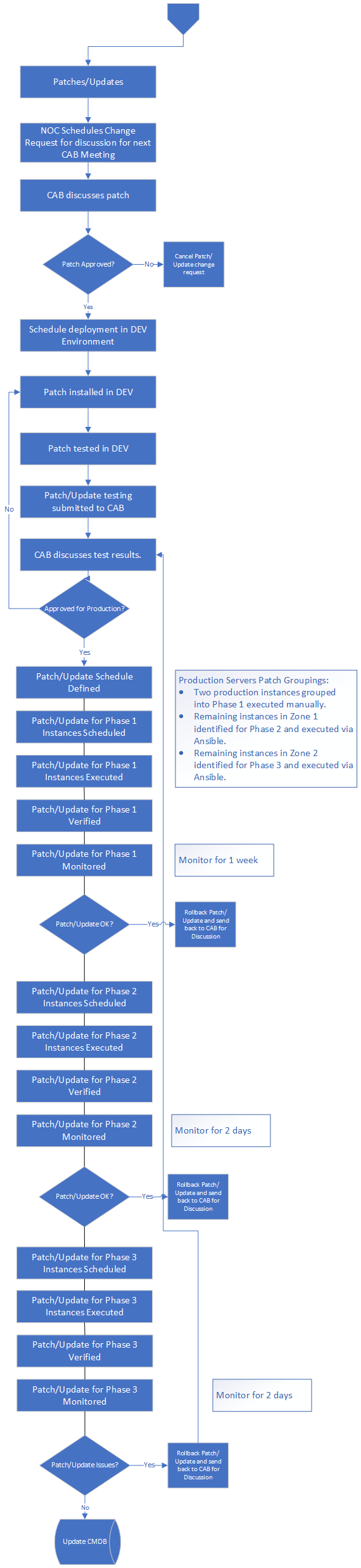


Table 6: Admin Access Sub-Process



Table 7: Magneto Create Account Sub-Process



Table 8: Windows Create Account Sub Process



Table 9: Customer Notification Sub Process



**Procedure 7.40.1 – Detailed User Creation Change Request**

**Description:** The Detailed User Creation Change Request process will detail the steps involved in order to create a new user account.

**Frequency**: After a user creation change request is made

**Prerequisites:**

1. New member joins the program

**Targets:** Systems

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a User Creation request |  |
| 3. | Customer approves account creation request |  |
| 4. | Request is approved by ISSO |  |
| 5. | Request is approved by the NOC Manager |  |
| 6. | Request is approved by PII Manager |  |
| 7. | Create account |  |
| 8. | Create Windows Account | Reference Windows Account Creation procedure |
| 9. | Add Windows Account to the appropriate groups |  |
| 10. | Assign user to a VDI server | 2 users can be assigned per server |
| 11. | Create Duo Account and send onboarding email |  |
| 12. | VPN Creation | <Need steps> |
| 13. | Create Google Account | Reference Google Account Creation procedure |

**Procedure 7.40.2 – GCP User Creation Change Request**

**Description:** The GCP User Creation Change Request process will detail the steps involved in order to create a user into our GCP environment.

**Frequency**: After a GCP user creation change request is made

**Prerequisites:**

1. New member joins the program

**Targets:** GCP

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a User Creation request |  |
| 3. | Customer approves account creation request |  |
| 4. | Request approved by ISSO |  |
| 5. | Request is approved by the NOC Manager |  |
| 6. | Request is approved by PII Manager |  |
| 7. | Create account |  |
| 8. | Create GCP Account |  |
| 8.1 | Sign into your Google Admin Console |  |
| 8.2 | Go to Users from the Admin console Home Page |  |
| 8.3 | Select the organizational unit you wish to add the user to |  |
| 8.4 | Click Add New User |  |
| 8.5 | Add Account Information | * First and Last Name * Enter External after last name if they are a contractor. * Enter a C after their last name if they are a customer. |
| 8.6 | Create Password | It can be autogenerated or manually created |
| 8.7 | Select Ask user to change password during next sign in |  |
| 8.7 | Click Add New User |  |
| 8.8 | Click Email User Sign-in info |  |
| 8.9 | Welcome email sent to user. User must reset their password within 48 hours |  |
| 9 | Does the user require admin privileges? |  |
| 9.1 | If Yes: Follow Admin Access procedure  If No: Proceed to Validate User can Login |  |
| 10 | Admin Access Procedure |  |
| 10.1 | Get NOC Manager approval |  |
| 10.2 | Sign into Google Admin console |  |
| 10.3 | Go to Users from the Admin console Home Page |  |
| 10.4 | Find user from the Users List |  |
| 10.5 | Click User’s name to open their account |  |
| 10.6 | Click Admin Roles and Privileges |  |
| 10.7 | Click Super Admin Role |  |
| 10.8 | Mark slider as Assigned |  |
| 10.9 | Click Save |  |
| 11 | Validate User can Login |  |
| 12 | Close the Change |  |

**Procedure 7.40.3 – Magneto User Creation Change Request**

**Description:** The Magneto User Creation Change Request process will detail the steps involved in order to create a new Magneto user account.

**Frequency**: After a magneto user creation change request is made

**Prerequisites:**

1. New member joins the program

**Targets:** Magneto

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a User Creation request |  |
| 3. | Customer approves account creation request |  |
| 4. | Request is approved by ISSO |  |
| 5. | Request is approved by the NOC Manager |  |
| 6. | Request is approved by PII Manager |  |
| 7. | Create account |  |
| 8. | Generate New ID | First 3 letters of first name  First 5 letters of last name  Numeric designator Eg: Geowashi01 (no duplicates of existing or previous accounts) |
| 9. | Generate initial password and set password to change during first login |  |
| 10. | Provide usernames via encrypted email |  |
| 11. | Provide one time pw in encrypted email |  |
| 12. | Assign user privileges |  |

**Procedure 7.40.4 – Windows User Creation Change Request**

**Description:** The Windows User Creation Change Request process will detail the steps involved in order to create a user and allowing them access into our Windows machines.

**Frequency**: After a Windows user creation change request is made

**Prerequisites:**

1. New member joins the program

**Targets:** Windows machines

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a User Creation request |  |
| 3. | Customer approves account creation request |  |
| 4. | Request is approved by ISSO |  |
| 5. | Request is approved by the NOC Manager |  |
| 6. | Request is approved by PII Manager |  |
| 7. | Create account |  |
| 8. | Login to Active Directory Users and Computers |  |
| 9. | Create User Account in Specified OU |  |
| 10. | Reference User Role and Active Directory Security Group Table in Appendix I |  |
| 11. | Enable Change Password at initial login |  |
| 12. | Ensure all fields are populated |  |
| 13. | Logon workstations need to be specified and the assigned VDI machine entered |  |
| 14. | Update Account Spreadsheet |  |

**Procedure 7.40.5 – Rollback Change Request**

**Description:** The Rollback Change Request process will detail the steps involved in order to revert the system back to a previous state before a change was implemented.

**Frequency**: After a rollback change request is made.

**Prerequisites:**

1. Previous change request

**Targets:** System

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a Rollback change |  |
| 3. | Submit to the CAB | Requires approval from the NOC manager and the Chief Engineer |
| 4. | Schedule the release |  |
| 5. | Implement the requested change |  |
| 6. | Post implementation review |  |
| 7. | Close the change |  |

**Procedure 7.40.6 – User Termination Change Request**

**Description:** The User Termination Request process will detail the steps involved in order to terminate users who have left the program or have been inactive for a certain period of time.

**Frequency**: After a user termination change request is made.

**Prerequisites:**

1. User termination
2. User has transferred
3. User has been inactive

**Targets:** Systems

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a User Termination change |  |
| 3. | Determine if this is regarding noncompliance with security policies |  |
| 3.1 | If Yes: Disable account and confirm Security Team is aware of noncompliance  If No: Proceed to account inactivity | Operations Team to disable account |
| 4 | Account Inactivity |  |
| 4.1 | Has the account been inactive for 60 days? |  |
| 4.2 | If Yes: Disable account  If No: Proceed to contractor step | Operations Team to disable account |
| 5 | Is the user a contractor? |  |
| 5.1 | If Yes: Disable and terminate account within 8 hours and notify vendor.  If No: Disable account for 30 days. After 30 days, terminate account | * Capture contractor company, contractor name and user ID in preexisting accounts list. * Both contractors and Deloitte employees must have their system access disabled within 8 hours of employment termination or project transfer. |
| 6 | Close the change |  |

**Procedure 7.40.7 – Patching/Updates Process**

**Description:** The Patching/Updates procedure will allow us to conduct approved software updates and necessary patches to our systems.

**Frequency**:

* After a patch/update change request is made.
* Patches are executed on Saturday evenings.

**Prerequisites:**

1. Software release/patch/update available

**Targets:** Servers/services

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted to Change Management team for approval | * Once submitted, it will sit in the Assessment stage until approved by the Change Management team to go onto CAB Approval |
| 2 | NOC Schedules Change Request for discussion for next CAB Meeting |  |
| 3. | CAB discusses patch |  |
| 4. | Patch Approved? |  |
| 4.1 | **If Yes:** Schedule deployment in DEV environment  **If No:** Cancel Patch/Update change request |  |
| 5. | Schedule deployment in DEV |  |
| 6. | Patch installed in DEV |  |
| 7. | Patch tested in DEV | When files are downloaded for patching, test to ensure the validation hash is ok. |
| 8. | Patch/update testing results submitted to CAB |  |
| 9. | CAB discussed test results |  |
| 10. | Approved for production? |  |
| 10.1 | **If Yes:** Patch/Update schedule defined  **If No:** Go back to DEV for further install and testing |  |
| 11. | Patch/Update Schedule Defined |  |
| 12. | Patch/Update for Phase 1 Instances Scheduled | Production Servers Patch Groupings:   * Two production instances grouped into Phase 1 executed manually. * Remaining instances in Zone 1 identified for Phase 2 and executed via Ansible. * Remaining instances in Zone 2 identified for Phase 3 and executed via Ansible. |
| 12.1 | Patch/Update for Phase 1 Instances Executed |  |
| 12.2 | Patch/Update for Phase 1 Verified |  |
| 12.3 | Patch/Update for Phase 1 Monitored | Monitor for 1 week |
| 13. | Patch/Update Ok? |  |
| 13.1 | **If Yes:** Go to Patch/Update for Phase 2 Instances Scheduled  **If No:** Rollback Patch/Update and send back to CAB for Discussion |  |
| 14. | Patch/Update for Phase 2 Instances Scheduled |  |
| 14.1 | Patch/Update for Phase 2 Instances Executed |  |
| 14.2 | Patch/Update for Phase 2 Verified |  |
| 1.3 | Patch/Update for Phase 2 Monitored | Monitor for 2 days |
| 15. | Patch/Update Ok? |  |
| 15.1 | **If Yes:** Go to Patch/Update for Phase 3 Instances Scheduled  **If No:** Rollback Patch/Update and send back to CAB for Discussion |  |
| 16. | Patch/Update for Phase 3 Instances Scheduled |  |
| 16.1 | Patch/Update for Phase 3 Instances Executed |  |
| 16.2 | Patch/Update for Phase 3 Verified |  |
| 16.3 | Patch/Update for Phase 3 Monitored | Monitor for 2 days |
| 17. | Patch/Update Issues? |  |
| 17.1 | **If Yes**: Rollback Patch/Update and send back to CAB for discussion  **If No:** Update CMDB |  |
| 18. | Update CMDB |  |

**Procedure 7.8 – Configuration Change Process**

**Description:** The Configuration Change process will detail the steps needed in order to approve any changes to our systems.

**Frequency**: After a configuration change request is made.

**Prerequisites:**

1. Baselines
2. Latest version of system

**Targets:** Systems

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a configuration request |  |
| 3. | Fill out form and submit to the Change Management group | * Once submitted, it will sit in the Assess stage until the Change Management group submits it for approval so that it may be reviewed by the CAB. |
| 3. | Is this an emergency change |  |
| 3.1 | If Yes: Submit to Emergency Committee for review  If No: Proceed to the CAB |  |
| 4. | Submitted to CAB for review |  |
| 5. | Change implemented in Development |  |
| 6. | Change is tested |  |
| 7. | Request to implement in Production |  |
| 7.1 | If request approved: Is this a major change?   * If Yes: Proceed to Customer Notification Process * If No: Proceed to Schedule Change   If denied: Go to Implement in Development | Customer Notification process will alert the customer of any major changes to the system. |
| 8. | Schedule change |  |
| 9. | Implement change |  |
| 10. | Perform Configuration Status Accounting |  |
| 11. | Conduct Configuration Verification and Audit |  |

**Procedure 7.40.8 – Software Installation Request**

**Description:** The Software Installation Request procedure outlines the steps needed in order to approve any software installations, both internal and from clients.

**Frequency**: Upon every software install request.

**Prerequisites:**

1. Software

**Targets:** VDI, VMs

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Software Installation request received | Client requests may be given to the designated Deloitte PM. They must then enter the request through ServiceNow. |
| 2. | NOC Manager reviews request |  |
| 3. | CAB approves request |  |
| 4. | Was the installation request from a client? |  |
| 4.1 | If Yes: proceed to notification step  If No: close change |  |
| 5. | Approval notification sent to the client | Deloitte PM will inform the client that the software request has been approved. |

**Procedure 7.40.9 – Client Software Installation**

**Description:** The Software Installation procedure outlines the steps in order to install software into the VDI machines.

**Frequency**: after every approved client software install request.

**Prerequisites:**

1. Approved Software Installation request

**Targets:** VDI

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Software implemented in development |  |
| 2. | Software install is tested |  |
| 3. | Request Prod deployment |  |
| 4. | Request approved? |  |
| 4.1 | If Yes: Schedule change  If No: Implement back in development |  |
| 5. | Implement change |  |
| 6. | Update CMDB |  |

**Procedure 7.41.0 – Post Implementation Process**

**Description:** The Post Implementation process will communicate completed changes to our stakeholders and update the CMDB.

**Frequency**: after a change request has been implemented.

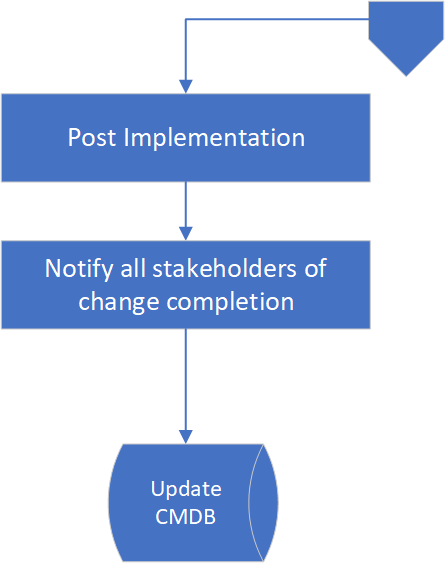
**Prerequisites:**

1. Completed changes

**Targets:** Stakeholders, SDD, CMDB

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Engineering review of change accuracy | NOC Manager will audit and review all configuration changes |
| 2. | Notify all stakeholders of change completion | Notify Deloitte PM of implemented change |
| 3. | Update SDD |  |
| 4. | Update CMDB of latest change |  |

Table 8: Post Implementation



# 8.0 Configuration Management

Our configuration management process is designed to keep up-to-date information about our assets and the component parts of the IT services we manage. The process ensures that accurate and reliable information about our assets are available when and where it is needed. All configuration changes will go through our Change Management process as stated in Section 8. ServiceNow (SNOW) will be our repository for housing all our documentation and images. Patches that are applied will be stored in SNOW unless the file is greater than 100MB. Those patches will need to be stored in a secure cloud storage bucket. As part of our improvement efforts, we shall conduct quarterly reviews of all configuration changes made.

## 8.1 Version control

The version control process will enable our team to track and manage different versions (or drafts) of a document so that everyone is aware of its current iteration. Users editing a document are required to update the Revision History table at the beginning of the document. Please be sure to enter the necessary information in the required fields so that everyone is aware of the changes that were made. When saving a new document, please be sure to use the approved NOC-nomenclature. If saving an existing document, please update the version.

## 8.2 Configuration Control Process

This section identifies the processes/steps required to ensure that all changes to D2C2 are properly requested, evaluated, and authorized. Processes provide detailed, step-by-step procedures for establishing, processing, tracking, and documenting changes.

The Configuration Control Process is critical to the D2C2 because of the number of changes, revisions, upgrades, and modifications that it is expected to undergo throughout its life cycle. Thus, the effective management of changes requires a formal, documented, systematic process for requesting, evaluating, tracking, and approving changes to the system.

## 8.3 Configuration Management Database (CMDB)

The Configuration Management Database will be used to store configuration records throughout their lifecycle. CMDB will store attributes of configuration items and their relationship with other configuration items. Any changes resulting from the Change Management process will be tracked in the CMDB. The CMDB will be housed in ServiceNow and include the following items:

* App Configuration Files
* The Solution Design Document

## 8.4 Logical Access Restrictions

The Logical Access Restriction Policy outlines how the NOC ensures that only authorized users with the required training and access execute configuration changes on this platform.

* All NOC personnel have been onboarded to the platform adhering to the User Creation process.
* Access to all systems managed by NOC personnel requires GCP IAM and MFA

# 9.0 Solution Design Document

The Solution Design document is provided as a separate standalone document.

# 10.0 User Access

Users requesting access into GCP will require approval through the change request process listed in the Change Management section. Upon being granted access, all users will use GCP IAM. For additional security measures, all Non-Deloitte System access accounts will have the word “external” listed in their username to quickly identify them as Non-Deloitte employees. Deloitte customers accessing the system will have a “C” listed in their username. All users will be needing MFA for system access. All user access will be supplied through preconfigured roles, and no permissions will be assigned to users.

## 10.1 User Password Policy

When creating a GCP password, users will have to adhere to the following policy:

* Strong password is enforced
* Password length minimum is set to 8 characters
* Strength and length will be enforced for every password change
* There will be enforced password policy at next sign-in
* Password reuse is NOT permitted
* Password reset frequency is set for 60 days

Table 9: GCP Password Policy



When creating a Windows password, users will have to adhere to the following policy:

* May not contain user’s account name or parts of the user’s full name that exceed two consecutive characters
* Password must be at least 8 characters in length
* Contain characters from three of the following four categories:
  + English uppercase characters (A through Z)
  + English lowercase characters (a through z)
  + Base 10 digits (0 through 9)
  + Non-alphabetic characters (for example, !, $, #, %)
* Complexity requirements are enforced when passwords are changed or created
* Enforce password reset every 40 days
* Password reuse allowed ONLY after 20 passwords

Table 10: Windows Password Policy



## 10.2 User Login Security Rules

Custom Google Security rule is implemented to suspend/lockout GCP user accounts for 60 minutes after

3 unsuccessful logins within a period of 60 minutes.

Windows GPO policy is implemented to suspend/lockout GCP user accounts for 30 minutes after 3 unsuccessful logins in 30 minutes.

## 10.3 User Password Recovery

**Procedure 10.3.1 – GCP Password Recovery**

**Description:** The GCP Password Recovery process outlines the steps taken by GCP users in order to recover their passwords due to them being forgotten or compromised.

**Frequency**: Whenever a password needs to be reset.

**Prerequisites:**

1. Created accounts

**Targets:** GCP

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Navigate to the GCP Sign-In Page |  |
| 2. | Click **Forgot Password** |  |
| 3. | Message displays to contact their administrator |  |
| 4. | User submits a ticket through ServiceNow | Please label the inquiry as Password Reset for GCP |

**Procedure 10.3.2 – GCP Password Recovery – Admin Steps**

**Description:** The GCP Password Recovery – Admin Steps process outlines the steps taken by GCP admins in order to reset a user’s password.

**Frequency**: Whenever a password needs to be reset.

**Prerequisites:**

1. User password reset ticket created through ServiceNow

**Targets:** GCP

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Sign into your Google Admin Console |  |
| 2. | From the Admin console Home Page, go to **Users** |  |
| 3. | In the **Users** list, find the user requesting a password reset |  |
| 4. | Hover over the user and click **Reset Password** |  |
| 5. | Select to automatically generate a password for the user |  |
| 6. | Click **Email Password** |  |

## 10.4 User Termination Reports

User termination reports will be communicated via email to the identified customer contact when users have been terminated or their accounts have been disabled.

## 10.5 User Inactivity

Windows session users will be disconnected from the system after 15 minutes of inactivity. Users may lock their workstations, but the 15-minute inactivity timer will disconnect all sessions. GCP Infrastructure session locks out after 60 minutes of inactivity.

Inactive GCP user accounts are manually disabled after inactivity of 35 days and deleted after inactivity of 120 days.

Users who have not logged into the system within two weeks will be marked as “inactive”. Restoring their access will require the below procedure:

Please reference procedures below:

|  |  |
| --- | --- |
| Procedure 7.3 | GCP User Creation Change Request |
| Procedure 7.4 | Magneto User Creation Change Request |
| Procedure 7.5 | Windows User Creation Change Request |

## 10.6 Privileged Access

Privileged command execution will be reviewed on a weekly basis. All privileged commands will be logged in ServiceNow.

## 10.7 User Access Review

User access will be reviewed on a yearly basis by the Change Control Manager. The Change Control Manager will also review admin access on a monthly basis.

# 11. Operational Maintenance

Our maintenance processes are established to sustain the capability of our systems in order to provide a superior service. Our processes monitor the system’s capability to deliver services, record problems for analysis, and take corrective, adaptive, and preventive actions. As a result of the successful implementation of the maintenance process, we are able to maximize system availability to meet the operational requirements.

The Network Operations Center (NOC) is responsible for managing the maintenance of our systems that live within our environment. Our team is comprised of engineers who are tasked to execute all maintenance activities. The Chief Engineer and the NOC Manager approve who is allowed to perform maintenance on our systems – this approval is granted through our user creation/account modification process. Members of our NOC team have the proper access and are U.S. Citizens. A list of personnel authorized to perform maintenance activities is found in Appendix K. Through our change management process, we are able to document and control all maintenance activities performed on our systems. The same process applies for all scheduled maintenance performed by our vendors. Our Maintenance Log (found in ServiceNow) will document all maintenance activities (both internal and external). External parties will be granted access to our systems through the user creation/account modification process and will have to authenticate through the D2C2 system process the same as internal administrators.

Our internal maintenance procedures include daily operational testing, reviewing critical incident logs, reviewing the performance of our systems from our logging and monitoring tasks and reviewing the results from our hourly health checks. The result of these activities will be logged in ServiceNow. Carrying out these checks ensures that our systems remain operational. All privileged activities in the system are audited by the appropriate monitoring agents and local system log monitoring tools. Audits are conducted by the NOC Manager and/or Shift Manager. In the event that maintenance support is needed, we have established Service Level Objectives with our partners in order to receive timely assistance regarding any support or maintenance request.

## 11.1 Daily Tasks



**Procedure 11.1.1 – Operational Testing Process**

**Description:** The Daily Operational Testing process will allow us to test that each application is operational.

**Frequency**: Performed hourly

**Prerequisites:**

1. Created application

**Targets:** Applications

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Open Nuance app |  |
| 1.1 | Validate that it is operational |  |
| 1.2 | Log operational status in ITSM SNOW |  |
| 2. | Open ServiceNow |  |
| 2.1 | Validate that it is operational |  |
| 2.2 | Log operational status in ITSM SNOW |  |
| 3. | Open BluePrism |  |
| 3.1 | Validate that it is operational |  |
| 3.2 | Log operational status in ITSM SNOW |  |
| 4. | Open Looker |  |
| 4.1 | Validate that it is operational |  |
| 4.2 | Log operational status in ITSM SNOW |  |

**Procedure 11.1.2 – Execute backup validate process**

Reference procedure 6.4

## 11.2 Maintenance Test and Diagnostic Tools

D2C2 has a formal approval process before introducing new software into the organization. Only tools on the approved software list (found in Appendix K) are scanned in Deloitte systems before they are introduced into the D2C2 environment.

# 12. Operational Activities

## 12.1 Daily Tasks

**Procedure 12.1.1 – Daily Stale Accounts Process**

**Description:** The Stale Accounts process will run a command in order to list stale accounts within the system.

**Frequency**: Daily

**Prerequisites:**

1. Created accounts

**Targets:** User Accounts

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Log into a power shell command line with elevated privileges |  |
| 2. | Execute the command - dsquery user -inactive 4 > staleaccounts.txt |  |
| 3. | Disable accounts listed in the staleaccounts.txt |  |

## 12.2 Weekly Tasks

**Description:** Conduct weekly change management meetings.



## 12.3 Monthly Tasks



**12.3.1 Review Admin Accounts process**

**Description:** Review admin accounts with security owners to validate system access.

**Frequency**: Monthly

**Prerequisites:**

1. Admin accounts

**Targets:** Admin accounts

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | NOC team to meet with Security team. | * Cadence can be every first Friday of every month. * NOC M to send out invite. |
| 2. | NOC Manager to pull a list of all active Admins within GCP. | Pull the Admin list from GCP. |
| 3. | NOC and Security team to review list and decide who no longer needs access or decide who will need to be granted access. | Granting or removing access will need to go through the CCB. |

## 12.4 Quarterly Tasks



**12.4.1 Review Authorized Software List**

**Description:** The CAB will review the Authorized Software List.

**Frequency**: Quarterly

**Prerequisites:**

1. Software List

**Targets:** Software

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | CAB to meet first week of every quarter | Establish what day of the quarter and make sure an invite is sent out to the respective members of the board. |
| 2. | Review updated version of the Software List | Software List can be found in Appendix: J |
| 3. | CAB will review list and make sure it is up to date. | NOC M will make any updates to the authorized list derived from these meetings. |

## 12.5 Yearly Tasks



**12.5.1 Review Access Agreements process**

**Description:** Procedure established to review access agreements.

**Frequency**: Yearly

**Prerequisites:**

1. Access agreements

**Targets:** Account access

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | NOC team to meet with Security team. | * Define who from our team will be present during these meetings. |
| 2. | Both teams will review the access agreements established. |  |
| 3. | Teams will determine which agreements need to continue and which need to be voided. |  |

**12.5.2 Review exceptions to the traffic flow policy**

**Description:** Procedure established to review exceptions to the traffic flow policy. Any exceptions found that are no longer supported by an explicit mission/business need will be removed.

**Frequency:** Yearly

**Prerequisites:**

1. Traffic Flow Policy

**Targets:** Systems

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Designated members of the NOC team and other appointees meet to review traffic flow policy. | * Determine who needs to be present during these meetings. * Determine when the meeting will be scheduled. * Have the NOC M send out the meeting invite. |
| 2. | Traffic Flow Policy is pulled from ServiceNow. |  |
| 3. | Members review the policy to find any exceptions. |  |
| 4. | Agreed upon exceptions will be removed from the policy. |  |
| 5. | [Policy owner] updates the policy to reflect the agreed upon changes. |  |
| 6. | Updated policy is uploaded into ServiceNow. |  |
| 7. | CMDB is updated. |  |

# 13.0 Vendor O&M

As our solution is comprised of multiple vendor integrations, we will (at times) require assistance from our partners in order to maintain a sustainable and operational environment. Should incidents arise that are outside of the D2C2 purview, NOC personnel will contact the respective vendor to which the incident corresponds. The below procedure outlines the proper steps on how to engage our partners during such incidents.

**13.1 Vendor Incident process**

**Description:** This process outlines how we are to communicate with our vendors should an incident arise that is outside of D2C2 control.

**Frequency**: As vendor related incidents occur

**Prerequisites:**

* 1. Incident ticket in ServiceNow is classified as a vendor issue

**Targets:** Production Systems

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Visit the vendor ticketing system that corresponds to the incident or outage | * If the vendor does not have a ticketing system that we can access, please reach out to the POC(s) in Appendix M * Be sure to be very detailed around the issue so that they have all the necessary information |
| 2. | Fill out incident form | Be sure to capture as many details as possible surrounding the incident. |
| 3. | Notify vendor POC(s) of reported incident or outage | Vendor POC list is found in Appendix M |
| 4. | Once the issue is resolved, close out the ticket in ServiceNow |  |

## 13.2 Vendor Incident Response Time

Similar to our own incident response timeframe, we also require our vendors to respond in a timely manner given the urgency of the incident. The below table outlines the priority of incidents and their response times:

|  |  |  |
| --- | --- | --- |
| **Priority** | **Description** | **Response Time** |
| P4 Issues | Non urgent, lower priority issues | Within 48 hours |
| P3 Issues | Support for important but not urgent issue | Within 24 hours |
| P2 Issues | Important and urgent issues that need to be addressed same day | Same day, within 1 hour |
| P1 Issues | Important and critical issues | Same day, within 15 minutes and treated as an all hands-on deck support issue with live support on the phone until the issue is resolved |

# 14.0 Document Maintenance

This SOP is a living document; updates will be added that clearly identify where in the life cycle that plan stands. The SOP will be reviewed at least semiannually but may be updated as needed. Subsequent to each incident event, whether actually or as part of the annual testing activities, a lessons learned analysis will be performed, and lessons learned that impact the content of this plan will be updated as required.

The SOP stresses mainly two fundamental principles. The first is the importance of following well-defined and systematic procedures to respond to network-related incidents. This program provides a sound set of considerations to use either verbatim or as a basis for developing custom procedures tailored to specific operational environments.

Even if incident response efforts are conducted systematically, they are of little value if conducted in isolation. The second principle, therefore, is that coordinating efforts with others is also a critical facet of incident response. For instance, sharing certain data can enable others to prevent or more quickly recognize and eradicate the cause of incidents.

# Appendices

## Appendix A: P1 Escalation List

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority** | **Time Limit Before Escalation** | **Escalate To** | **Name** |
| **P1** |  | NOC Manager  Chief Engineer  Include system SMEs  D2C2 ISSM  D2C2 ISSO  Customer |  |
|  |
|  |
|  |
|  |

## Appendix B: P2 Escalation List

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority** | **Time Limit Before Escalation** | **Escalate To** | **Name** |
| **P2** |  | NOC Manager  Chief Engineer  Customer |  |
|  |
|  |

## Appendix C: P3 Escalation List

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority** | **Time Limit Before Escalation** | **Escalate To** | **Name** |
| **P3** |  | NOC Manager  Chief Engineer  Customer |  |
|  |
|  |

## Appendix D: P4 Escalation List

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority** | **Time Limit Before Escalation** | **Escalate To** | **Name** |
| **P4** |  | NOC Manager  Chief Engineer  Customer |  |
|  |
|  |

## Appendix E: Contact List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role** | **Phone** | **Secondary Phone** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Appendix F: Log Review Form

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **User Identification** | **Event Type** | **Date & Time** | **Success or Failure Indication** | **Event Origination** | **Reference to the data, system component or resource affected** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Appendix G: Server Daily Backup Check

|  |  |  |
| --- | --- | --- |
| **Server** | **Project** | **Process** |
| BLP–IC–XX-A-W01 | BluePrism | * Log into console * Click File Store link * Go to Backups tab * Validate backup file date and time |
| BLP–RS–XX-A-W01 | BluePrism |
| BLP–AS–XX-A-W01 | BluePrism |
| BLP–IC–XX-B-W01 | BluePrism |
| BLP–RS–XX-B-W01 | BluePrism |
| BLP–AS–XX-B-W01 | BluePrism |
| LOK-OP-AS-A-L01 | Looker |
| LOK-OP-AS-A-L02 | Looker |
| LOK-OP-AS-A-L03 | Looker |
| LOK-OP-AS-A-L04 | Looker |
| LOK-OP-AS-B-L01 | Looker |
| LOK-OP-AS-B-L02 | Looker |
| LOK-OP-AS-B-L03 | Looker |
| LOK-OP-AS-B-L04 | Looker |
| SNO-WEB-AS-A-L01 | ServiceNow |
| SNO-WEB-AS-A-L02 | ServiceNow |
| SNO-WEB-AS-A-L03 | ServiceNow |
| SNO-WEB-AS-A-L04 | ServiceNow |
| SNO-WEB-AS-A-L05 | ServiceNow |
| SNO-WEB-AS-B-L01 | ServiceNow |
| SNO-WEB-AS-B-L02 | ServiceNow |
| SNO-WEB-AS-B-L03 | ServiceNow |
| SNO-WEB-AS-B-L04 | ServiceNow |
| SNO-WEB-AS-B-L05 | ServiceNow |
| SNO-MAN-AS-A-L01 | ServiceNow |
| SNO-MAN-AS-B-L01 | ServiceNow |
| nua-nb-lb-a-w01 | Nuance |
| nua-nb-mn-a-w01 | Nuance |
| nua-nb-mn-b-w02 | Nuance |
| nua-nb-mn-a-w03 | Nuance |
| nua-nb-mn-b-w04 | Nuance |
| nua-nb-vp-a-w01 | Nuance |
| nua-nb-vp-a-w02 | Nuance |
| nua-nb-vp-a-w03 | Nuance |
| nua-nb-vp-a-w04 | Nuance |
| nua-nb-vp-a-w05 | Nuance |
| nua-nb-vp-a-w06 | Nuance |
| nua-nb-vp-a-w07 | Nuance |
| nua-nb-vp-a-w08 | Nuance |
| nua-nb-vp-a-w09 | Nuance |
| nua-nb-vp-a-w10 | Nuance |
| nua-nb-vp-a-w11 | Nuance |
| nua-nb-vp-a-w12 | Nuance |
| nua-nb-vp-a-w13 | Nuance |
| nua-nb-vp-a-w14 | Nuance |
| nua-nb-vp-a-w15 | Nuance |
| nua-nb-vp-a-w16 | Nuance |
| nua-nb-lb-b-w01 | Nuance |
| nua-nb-mn-b-w01 | Nuance |
| nua-nb-mn-b-w02 | Nuance |
| nua-nb-mn-b-w03 | Nuance |
| nua-nb-mn-b-w04 | Nuance |
| nua-nb-vp-b-w01 | Nuance |
| nua-nb-vp-b-w02 | Nuance |
| nua-nb-vp-b-w03 | Nuance |
| nua-nb-vp-b-w04 | Nuance |
| nua-nb-vp-b-w05 | Nuance |
| nua-nb-vp-b-w06 | Nuance |
| nua-nb-vp-b-w07 | Nuance |
| nua-nb-vp-b-w08 | Nuance |
| nua-nb-vp-b-w09 | Nuance |
| nua-nb-vp-b-w10 | Nuance |
| nua-nb-vp-b-w11 | Nuance |
| nua-nb-vp-b-w12 | Nuance |
| nua-nb-vp-b-w13 | Nuance |
| nua-nb-vp-b-w14 | Nuance |
| nua-nb-vp-b-w15 | Nuance |
| nua-nb-vp-b-w16 | Nuance |

## Appendix H: Database Daily Backup Check

|  |  |  |
| --- | --- | --- |
| **Database Server** | **Project** | **Process** |
| BLP–DB–XX-A-W01 | BluePrism | * Log into console * Click File Store link * Go to Backups tab * Validate backup file date and time |
| BLP–DB–XX-B-W01 | BluePrism |
| SNO-WEB-DB-A-L01 | ServiceNow |
| SNO-WEB-DB-B-L01 | ServiceNow |
| SNO-MAN-DB-A-L01 | ServiceNow |
| SNO-MAN-DB-B-L01 | ServiceNow |
| LOK-OP-DB-A-L01 | Looker |
| LOK-OP-DB-B-L01 | Looker |

## Appendix I: Filestore Daily Backup Check

|  |  |  |
| --- | --- | --- |
| **Filestore** | **Project** | **Process** |
| Magneto Looker Filestore | Looker | * Log into console * Click File Store link * Go to Backups tab * Validate backup file date and time |
| Magneto Nuance Filestore | Nuance |
| Magento ServiceNow Filestore | ServiceNow |
| Magneto BluePrism Filestore | BluePrism |

## Appendix J: User Role and Active Directory Security Group

|  |  |
| --- | --- |
| **User Role** | **Active Directory Security Group** |
|  |  |
|  |  |

## Appendix K: Software Approved List

## 

|  |  |  |
| --- | --- | --- |
| **Software** | **Version in Production** | **Notes** |
| ServiceNow | Quebec | Software in the environment |
| Blue Prism | v6.10.1 | Software in the environment |
| Nuance | v12.2.0 | Software in the environment |
| Looker | v21.4.22-fff155 | Software in the environment |
| Windows Active Directory | v10.0.17763.1697 | Software in the environment |
| Windows Server | 2019 Server | Software in the environment |
| RHEL Server | v7 and 8 | Software in the environment |
| Debian Server | v10 Buster | Software in the environment |
| Mariah DB and MySQL | v10.2 | Software in the environment |
| Google Workspaces - Business Standard |  | Google Services Consumed |
| Cloud Identity Premium |  | Google Services Consumed |
| Identity-Aware Proxy |  | Google Services Consumed |
| Cloud IAM |  | Google Services Consumed |
| CCAI/ DialogFlow CX |  | Google Services Consumed |
| Cloud Domains |  | Google Services Consumed |
| Cloud DNS |  | Google Services Consumed |
| Cloud SQL – MySQL |  | Google Services Consumed |
| Cloud Storage |  | Google Services Consumed |
| Filestore |  | Google Services Consumed |
| Global Load Balancer |  | Google Services Consumed |
| VPC |  | Google Services Consumed |
| Cloud Logging |  | Google Services Consumed |
| Cloud Pub/Sub |  | Google Services Consumed |
| Cloud Monitoring |  | Google Services Consumed |
| Cloud VPN |  | Google Services Consumed |
| Google Compute Engine |  | Google Services Consumed |
| Security Center |  | Google Services Consumed |
| BigQuery |  | Google Services Consumed |
| Splunk | v7.3.3.0 x64 | SOC |
| Tanium | v7.4.4.1250 | SOC |
| McAfee | 5.7.1.116 | SOC |
| Tenable.io | vNessus Agent 8.2.4-x64 | SOC |
| Palo Alto |  | IPS |
| Digicert |  | CA |
| DUO |  |  |

## Appendix L: Authorized Maintenance Personnel

|  |  |
| --- | --- |
| **Name** | **Role** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Appendix M: Vendor POC List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vendor Name** | **Contact Name** | **Role** | **Phone Number** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Appendix N: Change Roles

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Process Role** | **Phone Number** | **Email** |
|  | Change Process Owner |  |  |
|  | Change Manager(s) |  |  |
|  | Change Owner/Coordinator |  |  |
|  | Change Indicator |  |  |
|  | Change Implementer |  |  |
|  | CAB/ECAB Member |  |  |
|  | CAB/ECAB Chair |  |  |