PNU IT

Availability Management Policy

Version: 1.2

جامعة الأميرة نورة بنت عبدالرحمن
Princess Nourah Bint Abdulrahman University
PNU, Saudi Arabia

Reviewers

Name	Role	Comments	Date
Mohd. Tahseen	Process Owner PNU IT		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	14/08/2012	First Draft – Created by Surjajyoti Chowdhury
1.0	04-10-2015	Baselined
1.1	15-10-2015	Change C1004446
1.2	06-May-2020	Updated new Logo , Updated PNU management.

Referenced Documents

The following documents should be read in conjunction with this document:

Name	Version	Location

1 Introduction

The objective of this document is to detail out the guidelines to govern Availability Management process. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the Availability Management process in the organization

2 Scope

The scope of this process covers the design, implementation, measurement and management of IT service and infrastructure availability. The Availability Management ensures that all the services and components are designed and delivered in a cost justified manner to meet their targets as per agreed business needs. It aims to provide:

- A structured approach to availability
- Understanding of business requirements vs IT capability
- Understanding of service risks through use of tools
- Improved business perception
- Understanding of business planning

The Availability Management process has two key elements:

Proactive Activities

Services should be designed and built to meet the business requirements, defined as part of the project process and controlled via Service Introduction/Service Transition. This is the accountability of the project team who should agree availability targets with the owning business/customer and Service Management teams.

Reactive Activities

Maintaining availability levels within agreed targets through understanding current levels, incidents, problems, IT and business change plans.

The process aims are:

- Monitoring of all aspects of availability, reliability and maintainability of IT services and supporting components
- Maintenance of a set of methods, techniques and calculations for all metrics and reporting
- Assistance with risk assessment and management activities
- Production of availability reports
- Understanding and agreeing current and future demand (i.e business change requirements)
- Influencing the design of services to meet business availability requirements
- Assistance with the identification and resolution of any incidents and problems associated with service unavailability
- Proactive improvement of service availability

- Ensuring that IT is capable of delivering to its agreed service level agreements (SLAs)

Out of Scope

The Availability Management process does not include Business Continuity Management and the resumption of business processing after a major disaster.

Assumptions

- Access to SLAs, SLRs, OLAs and underpinning contracts is available
- Access to details of CIs or the CMDB
- Supporting and interfacing process are defined and implemented.

3 Policy Description

The policies for Availability Management at PNU IT are as follows:

- Assess and document the risks to availability of services
- Identify service availability requirements taking into consideration business plans, service requirements, SLAs, risks and impact of non-availability.
- Define the availability and recovery design criteria and service recovery procedure
- Produce, implement and update the service availability plans.
- Review the availability plan at least annually to ensure that requirements are met as agreed in all circumstances from normal through to a major loss of service
- These plans shall be maintained to ensure that they reflect agreed changes required by the business.
- Changes to these plans shall be controlled by the change management process
- The availability plan shall be re-tested at every major change to the business environment
- Availability shall be measured and recorded. Unplanned non-availability shall be investigated and appropriate actions need to be taken
- The Service Availability process shall adhere to existing security policies and procedures along with other regulatory requirements

4 Acronyms

Acronym	Description
ECAB	ECAB Emergency Change Advisory Board
CSI	Continual Service Improvement
DC	Data Center
EUSS	End User Service Support
IT SMS	Information Technology Service Management System

ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
KEDB	Known Error Database
NOC	Network Operations Center
OLA	Operational Level Agreement
PNU	Princess Noura Bint Abdulrahman University
RFC	Request for Change
CAB	CAB Change Advisory Board
AVM	Availability Management

PNU IT

Configuration Management Policy

Version: 1.2

PNU, Saudi Arabia

Reviewers

Name	Role	Comments	Date
Madhu Babu Allu	Process Owner		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	07/09/2012	First Draft – Created by Surjajyoti Chowdhury
1.0	20/03/2012	Baselined from draft version 0.1
1.1	16/07/2018	Removed wipro logo and completed annual review – Change Manager
1.2	06/05/2020	Updated new Logo and New PNU Management

Referenced Documents

The following documents should be read in conjunction with this document:

Name	**Version**	**Location**

1 Introduction

The objective of this document is to detail out the guidelines to govern Configuration Management process. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the Configuration Management process in the organization

2 Purpose

Configuration control covers the update of CI records in the CMDB to reflect authorized changes in the PNU IT Infrastructure. This document describes the policy that governs the distribution of authorization within PNU IT Operations to update CI records in the CMDB.
Configuration control activities depend on change management inputs. Consequently, the Configuration Management Authorization policy follows the design of the change management process.

3 Scope

This section specifies the scope of Service Configuration Management in terms of several dimensions. When interpreting these statements:

- Where there may be overlapping 'In' and 'Out' of scope statements, the default assumption is that the 'out' statement has precedence unless explicitly specified otherwise.
- Where there is not an 'in-scope' statement that applies, the principle is considered out of scope (i.e. the 'Out of scope' statements are specified cases for clarity only, and are not designed to be exhaustive).

3.1 Scope by Supported Process

In Scope

- The scope of information is limited to that which is required to support the following IT Service Management processes:

  - Incident Management Process
  - Problem Management Process
  - Service Request Fulfilment Process
  - Change Management Process
  - Release and Deployment Process

- The information is limited to that required in order to enable their process workflow, and not necessarily the technical detail of any given scenario. E.g. if a Problem Management investigation relates to insufficient capacity and performance, then:
  - Information required to enable generic Problem Management workflow is considered in-scope (e.g. specifying the affected services or components etc.);

- Information required to analyse the specific capacity and performance issues (e.g. capacity requirements, usage trending etc.) is considered out-of-scope (i.e. it is assumed to come from a specific Capacity and Performance information source).
- All Systems Management requirements, such as information regarding:
    - Technical Specification.
    - Technical Configuration: e.g. details on the 'settings' of an IT component;
    - Document Management
- Asset Management: e.g. for managing an inventory of IT Components deployed, in stock, order or disposed of;
- Release Management activities for Software and Content, such as retaining software baselines, applying changes to the configuration 'settings' of any IT component such as servers and application software etc;
- Release Management activities for Hardware, such as applying asset tags, etc.
- Service Configuration Management aims to identify components and their relationship to IT Service. Hence, the relationships within scope are hierarchical.

Out of Scope

- Knowledge Management (i.e. relating to 'How to' queries, and self-help facilities)
- Document Management
- Physical Controls: such as access to data centres, managed tech rooms, cabinets etc.
- Logical controls: such as the control of user accounts, passwords, privileges etc.
- Real-time alerting: Information regarding the real-time status of an item is considered out-of scope.
- Capacity and Performance Management: e.g. the provision of Capacity and utilisation data, physical logistics of physical Logistics of hardware installations
- Cost Management: including cost recovery, recharging etc.
- Software Licence Compliance.

3.2 Scope by Item Types

In Scope:

- The item types specified in Appendix 1 are considered currently in scope. These can be summarised for ease of understanding:
    - IT Services
    - Systems
    - Corresponding 'logical' computer types (such as partitions etc.);
    - Server, Storage Hardware of all types;
    - Firewalls

Out of Scope:

- All other item types are considered out of scope.

4 Policy Description

Implementation of changes can involve the deployment of new service and infrastructure components as well as the modification of existing ones. The Configuration Authorization policy is different in each case.

4.1 Data Ownership

All Data shall have an agreed data owner, who is accountable for maintaining the completeness, correctness and currency of the data.

4.2 Initial registration

The implementation of new service and infrastructure components requires the identification and initial registration of the Configuration Items (CIs) that are part of the new service and infrastructure components. ***Identification and initial registration of CIs is described in the Configuration Identification Procedure.***

To protect the integrity of the data model of the CMDB, the authorization for the identification and initial registration of CIs is restricted to the Configuration Administrator.

4.3 Updating existing CI records

To reduce the workload of the Configuration Manager, authorization to update existing CI records can be transferred to Configuration Management Administrator.

The authorization to update existing CI records only applies to those changes specified in the authorized change request. Compliance with this provision will be monitored under the Configuration Verification procedure on the basis of automatically generated record change logs.

Delegation of authorization to Configuration Administrator requires proper training and clear work instructions on how to use the tool

4.4 Unknown' and 'Not Applicable' Information

Where data is not known or not applicable, it is the policy to provide, where appropriate, the means by which this can be recorded. For example, if the state of an item is unknown, the system will provide the data owner with the means to specify the status as 'Unknown'.

It is intended that this provision:

- Enables data incompleteness to be identified and measured;
- Enables greater confidence in complete data, insofar as it is less likely to be polluted with 'guesses' or estimated values.

5 CMDB Access rights

Access rights to the CMDB comprise view rights and edit rights. These rights can be attributed to specific parts of the CMDB. Access rights can be restricted to:

- CI category
- CI types within CI categories
- CI User, administrator or owner
- Any combination of the above

PNU IT staff can be granted access rights depending on their role and/or function.

The Configuration Administrator must maintain a list of access rights relevant to all roles and functions within PNU IT Operation. The Configuration administrator is responsible for the CMDB user administration in compliance with the access right on this list.

6 References

None

7 Acronyms

Acronym	Description
ECAB	ECAB Emergency Change Advisory Board
CI	Configuration Item
SBG	Saudi Bin Laden Group
SBM	Saudi Business Machine
IT SMS	Information Technology Service Management System
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
CMDB	Configuration Management Database
NOC	Network Operations Center
PNU	Princess Noura Bint Abdulrahman University
RFC	Request for Change
CAB	CAB Change Advisory Board
SO	SAUDI OGER LTD

8 Appendices

Appendix 1: Item Types in Scope

Type	Sub Type
Hardware.Server	Linux
	Windows
	Unix
	Other Server
Hardware.Virtual Machine	VMWare
	Other Hardware Virtual Machine
Hardware.Other	Other Hardware
	Network Printer
Hardware.Storage	Disk Array
	Disk Expansion
	Hard Drive
	Network Attached Storage
	Storage Area Network
	Tape Unit
	Tape Library
	Virtual Tape System
Hardware. Workstation	VDI
	Laptop
	Desktop
Network.Switch	Network Switch
SAN.Switch	Switch
Network.Router	Router
Network.Other	Other Network devices
	IPS (Intrusion prevention system)
	Firewall
	Load Balancer
Software.Application	Application
Software.Operating System	HP UX OS
	Linux OS
	Unix OS
	Windows OS
	Vmware OS

	Other Software OS
Software.Database	Oracle
	SQL
	Other Software Database
Hardware.EndUserComponent	ePodium
	IP Phone
Service	As per Service Catalogue

Appendix 2– PNU IT user authorization table

Configuration Management Role	**View**	**Edit**
Configuration Manager	CMDB	CMDB
Service Support Staff (Service Desk)/ L1/ L2/ L3/ Domain Leads	All CIs	No Edit rights
Configuration Management Administrator	All CIs	▪ All CIs ▪ Reference Tables

PNU IT

Change Management Policy

Version: 1.2

جامعة الأميرة نورة بنت عبدالرحمن

Princess Nourah Bint Abdulrahman University

PNU, Saudi Arabia

Reviewers

Name	Role	Comments	Date
Ahsan Bashir	Documentation Process Owner		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	15/11/2012	First Draft – Created by Surjajyoti Chowdhury
1.0	20/02/2013	Baselined from draft version 0.1
1.1	16-Jul-2018	Removed Wipro logo and completed annual review – Change Manager
1.2	06-May-2020	Updated new Logo , Updated PNU management.

Referenced Documents

The following documents should be read in conjunction with this document:

Name	Version	Location

1 Introduction

The objective of this document is to detail out the guidelines to govern Change Management process. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the Change Management process in the organization

2 Scope

This document describes the policy for the Change Management process. These principles will guide the process in execution from beginning to end through the organisational environment of infrastructure and application support.

Change is defined as the addition, modification or removal of service/s or any Configuration Items that could have an effect on the Services of PNU IT. Thus change management includes all IT Services, Configuration Items, ITSM Processes and their Documentation.

The scope of change management covers:

- The CIs which are defined under CMDB are scoped for within the Change Management Process
- All changes to a service or service components
- Transfer of a service from the service provider to the production environment
- Removal of a service

This document covers the following change types adopted at PNU IT:

- **Standard change** is a change to for which the approach is pre-authorized by Change Management, has an accepted and established procedure to provide a specific change requirement. Some standard changes will be triggered by the request fulfilment process and be directly recorded and passed for action by the service desk. E.g. of Standard Changes are like New Media Configuration, New Tape Library Installation, CTI Route configuration, etc.

The key points to note which constitute a standard change:

- *Negligible Risk*
- *Guaranteed No Service Impact, even if change fails*
- *Proven, consistent and regular activity*
- *No Financial impact from change*
- *All Implementation activities carried out by the technical team that own the change without any additional approvers or supporting teams required.*
- *All Standard changes must be agreed with Change Advisory Board prior to their use*

These characteristics can be applied to convert a Normal change to a standard change with the approval of the CAB.

- **Emergency change** is a Change due for implementation as soon as possible of the record being raised. Emergency changes are raised to fix a failed activity in response to an incident within the live production service or to prevent a potential failure within the live production service, where potential for that failure is immediate. The related approvals and documentation are updated later, after the emergency change is implemented.

  Characteristics of an emergency change are:

  - Urgency to effect the change is critical
  - Impact on the customer or service is critical
  - Risk to the customer or service critical
  - Risk of failure or degradation to IT Services

  Such emergency changes shall be passed to ECAB for approval. Approvals can be taken on call/mailer depending on the urgency and availability of ECAB members.

- **Normal change** is a change that follows all of the steps of the change process. It is assessed by the Change Manager. This assessment is further reviewed and discussed by CAB. Normal Change is segregated into major, significant and minor as per their impact.

  - **Major Change** is a change that has major impact on customer or services. Removal of a service or Transfer of a service will be categorized as a major change and is handled through the process Design and Transition of New or Changed Services.

    The criteria to determine changes with potential to have a major impact on services or the customer are:

    - The removal of a service
    - Addition of a new service
    - The transfer of a service from the service provider to the customer or a different party
    - Any change that is assessed to have a major impact as part of the change management process
    - Changes to projects are managed by the project change request procedure and recorded in the project change register

  - **Significant Change** is defined as a medium risk, involving complex changes altering production systems and difficulty with backup/recovery in the event of an issue. Significant changes require review and approval at the Change Advisory Board (CAB) meeting prior to implementation. E.g.System Configuration - Adding server, Router IOS Crash, etc

- **Minor Change** - Defined as a low risk change, categorized by limited impact to production/ Live IT services enviroment, and the ability to adequately test prior to implementation and easily back-out/recover in the event of an issue. Minor changes require review and approval by the Change Manager and if required by the technology manager of the group performing the change. Only if the Change Category is Minor, the Change Manager can authorize and schedule the RFC without involvement of the CAB. E.g. Disk Installation, Firmware / Bios Upgrade, etc

Out of Scope

- Changes with significantly wider impacts than service changes. Some examples are changes to departmental organization, policies and business operations.
- Changes at an operational level such as repair to printers or other routine service components.
- Changes pertaining to Non-IT services

3 Policy Description

- Changes shall be classified, recorded, validated, accepted and prioritized.

3.1 Principles confirming the acceptance of corporate policies, Regulatory policies on Governance and Service Management

- The Change Management process shall adhere to PNU IT Service Management policies and shall be based on the needs of the business
- The Change Management process shall adhere to existing security policies and procedures along with other regulatory requirements

3.2 Principles confirming Customer Focus

- Change Management process shall establish standardized methods and procedures for efficient and prompt handling of all changes and aim for minimum disruption to the services to the customers.
- Definition of Emergency Change should be agreed with University and documented
- Change Management process shall ensure that the changes are communicated to the University as per the communication plan defined in the Change Management Work Instructions.

3.3 Principles on Activities with Controls on the process

- Change Manager shall be an identified person accountable for the change management process.
- All changes to a service or service component shall be raised using a request for change. Change Manager in discussion with CAB members should take the decisions on accepting a particular Request for Change
- All change requests shall include business benefit, risk assessment, impact analysis and roll back details
- Change Management process shall:
    - Establish the criteria to determine changes with potential to have a major impact on services or the customer.
    - Classify the removal of a service as a change to a service with the potential to have a major impact.
    - Classify the transfer of a service from the service provider to the customer or a different party as a change with potential to have a major impact
    - Establish that approved changes are developed and tested.

- The change shall be reversed or remedied if unsuccessful. Unsuccessful changes shall be investigated and agreed actions taken.
- Establish that schedule of change containing details of the approved changes and their proposed deployment dates is established and communicated to interested parties.

- Significant, Major, Emergency changes shall be reviewed after implementation and for any post implementation action. Minor Change if requires will go through Review process. Emergency Change should be reviewed within 72 hours of implementation.
- A review board shall review the changes periodically to assess the trends and improvement areas.
- The findings of the review board shall be documented, published and shall form an input to the service improvement plan.
- The impacted configuration items shall be updated in the CMDB on implementation

4 Acronyms

Acronym	Description
ECAB	ECAB Emergency Change Advisory Board
CSI	Continual Service Improvement
DC	Data Center
EUSS	End User Service Support
IT SMS	Information Technology Service Management System
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
KEDB	Known Error Database
NOC	Network Operations Center
OLA	Operational Level Agreement
PNU	Princess Noura Bint Abdulrahman University
RFC	Request for Change
CAB	CAB Change Advisory Board
CHM	Change Management

PNU IT

Capacity Management Policy

Version: 1.3

PNU, Saudi Arabia

Reviewers

Name	Role	Comments	Date
Shaik Shameeulla	Process Owner		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	21/09/2012	First Draft – Created by Surjajyoti Chowdhury
1.0	07/10/2013	Baselined from sign off draft version 1.0
1.1	10/12/2015	Updated the procedure and uploaded the approved version by Saroja Kumar Behera
1.2	01/06/2018	Removed logo and completed annual review
1.3	06/05/2020	Updated new PNU logo and New PNU Management.

Referenced Documents

The following documents should be read in conjunction with this document:

Name	Version	Location

1 Introduction

The objective of this document is to detail out the guidelines to govern Capacity Management process. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the Capacity Management process in the organization

2 Scope

The Capacity Management process applies for the IT support within the scope of PNU IT ensuring necessary Capacity is available at all times.

- Identify Capacity Requirements
- Review existing Capacity
- Prepare Capacity plan(s) based on forecasts
- Implement Capacity plan(s)

Out of Scope

- Services not part of Service Catalogue

3 Policy Description

The policies for Capacity Management at PNU IT are as follows:

- The Capacity Management process shall identify Capacity requirements on the basis of business plans, business requirements, SLAs and risk assessments, and shall be consulted in the development and negotiation of SLA's

- Capacity Plans will be kept on file for 18 months after their expiry date

- The Capacity Plans will be reviewed at least annually to ensure requirements reflect agreed-upon changes required by the business

- The Capacity Management process will be subject to Continuous Process Improvement

- Capacity Management will endeavor to ensure optimal integration with other ITSM processes

- The best available demand forecasts should be provided to Capacity Management as soon as they are identified

- Monitoring, data gathering, analysis, reporting, and reviews will be undertaken consistently in a defined manner, with the data being stored in the Capacity Management Database (CDB)

- The contents of the CDB will be shared with other ITSM processes

- The necessary authority will be delegated to the Capacity Management process to initiate actions which ensure required levels of IT Service Capacity and reliability

- The Capacity Plan shall include time frames, costs and thresholds
- The Capacity plan shall be prepared and reviewed periodically based on Business and Performance needs
- Changes to the capacity plan shall be controlled by the change management process
- The Capacity plan shall analyze impacts of service upgrades, technology changes, external changes and change requests

4 Acronyms

Acronym	Description
ECAB	ECAB Emergency Change Advisory Board
CSI	Continual Service Improvement
DC	Data Center
EUSS	End User Service Support
IT SMS	Information Technology Service Management System
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
KEDB	Known Error Database
NOC	Network Operations Center
OLA	Operational Level Agreement
PNU	Princess Noura Bint Abdulrahman University
RFC	Request for Change
CAB	CAB Change Advisory Board
CHM	Change Management

PNU IT

Incident Management Policy

Version: 1.2

Reviewers

Name	Role	Comments	Date
Mohammed Mudassir Niaz	Process Owner		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	03/11/2011	First Draft – Created by Bhavesh Bijagare
0.2	27/07/2012	Second Draft – Created by Surjajyoti Chowdhury
1.0	20/02/2013	Policy Baselined from sign off draft version 0.2
1.1	10-07-2018	Removed logo and reviewed
1.2	06/05/2020	Updated new PNU logo and new PNU management.

Referenced Documents

The following documents should be read in conjunction with this document:

Name	**Version**	**Location**

1 Introduction

The objective of this document is to detail out the guidelines to govern Incident Management processes. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the Incident Management process in the organization

2 Scope

These principles will guide the process in execution from beginning to end through the organizational environment of infrastructure and application support

The full end-to-end lifecycle of an incident record is included in the scope e.g. from the Incident being recorded in the designated tool to service, through to service being restored with either a permanent or temporary fix and the incident record being closed.

The scope of the Incident Management process therefore encompasses the IT Service Desk, L1 Support Group, L2 Support Group, L3 Support Group, Incident Management and subsequent interfaces with Third Party support.

Incident Management process in its current form will restore agreed service levels within agreed service levels to obtain the highest possible stability in IT service delivery, will work proactively and reactively to restore service as soon as possible when incidents occur and to feed into the Problem Management process so as to reduce the number of incidents in the future.

3 Incident Management Process

Incident Management is the process responsible for managing the lifecycle of all reported incidents. The primary objective of Incident Management is to provide a consistent method for recording and tracking incidents until they are closed

4 Process Governance Principles

4.1 Acceptance to Corporate Policies & Regulatory Policies

- The Incident Management process shall adhere to IT Service Management policies and shall be based on the needs of the University
- The Incident Management process shall adhere to existing security policies and procedures along with other regulatory requirements

4.2 Customer Focus

- Incident Management shall direct its efforts to minimize the impact of incidents on the University by restoring service as quickly as possible within the agreed service levels, in a cost-justifiable way and meet Customer Expectations

4.3 Process Control

- The Incident Management shall define procedures to handle Incidents
- Incident Management Process shall include
  - Recording
  - Allocation of priority
  - Classification
  - Updating of records
  - Escalation
  - Resolution
  - Closure
- The Incident Management process shall in conjunction with business agree on the definition of Major Incident
- Priority of Incidents should be determined based on Impact and Urgency of the Incident
- Major incidents should be classified and managed according to a documented procedure
- Top management shall be informed of Major Incidents and once major incident has been resolved, it should be directed to Problem Management for a review
- Major Incident Review report with recommendation identifying opportunities for improvement should be submitted within 72 Hours of Incident closure
- The Incident Management process shall do process performance reporting

4.4 Establishing Incident Management in the organization

- **Establishing Roles and responsibilities**
  The Incident Management process shall define roles and responsibilities to manage the maintain (viz. Incident recording, classification, diagnosis, solution and workaround creation and escalation) the process and its relationship with other service management processes
- **Establishing Tools usage**
  Incident Management process shall identify tools to be used for Incident recording till closure
- **Establishing Communication and Reporting**
  Incident Management shall have pre-defined communication channels for coordinating with cross functional groups, vendors, senior management and to handle escalation
- **Establishing Skill Update structure**
  Incident Management process shall perform skill benchmarking of its entire staff to understand the knowledge and training requirement to run and manage the process. Process shall build skill update plan and report the progress against the plan
- **Establish Process Relationship**

The Incident Management shall create a relationship map and relationship extent with all the service management process in scope

- **Escalation and Conflict Management**
  The Incident Management process shall have pre-defined escalation matrixes for all IT services. Process shall update and publish the details of these matrixes at appropriate intervals

4.5 Compliance Management

- The Incident Management process shall measure the compliance and also connect compliance findings to service improvements
- The Incident Management process shall follow organization wide audit and compliance process, if applicable

4.6 Process Review & Improvement

- Incident Management process shall review and validate the process regularly with all its stakeholders including tailoring requirements
- Incident Management process shall seek management review on principles of process governance
- Incident Management process shall provide all inputs to central process management function and process architecture unit for centralized process management

5 Acronyms

Acronym	Description
CMDB	Configuration Management Database
DC	Data Center
EUSS	End User Service Support
ICM	Incident Management
IT SMS	Information Technology Service Management System
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
KEDB	Known Error Database
NOC	Network Operations Center
OLA	Operational Level Agreement
PNU	Princess Noura Bint Abdulrahman University for Women
RFC	Request for Change
SLA	Service Level Agreement
UC	Underpinning Contract

Princess Nourah Bint Abdulrahman University **Document Number** PNU ITSM ITSCM 20 003	ITSCM Management Policy		
	Issue Date **06-May-2020**	**Effective On** **08-May-2020**	**Internal**

PNU IT

IT Service Continuity Management Policy

Version: 1.2

جامعة الأميرة نورة بنت عبدالرحمن
Princess Nourah Bint Abdulrahman University

PNU, Saudi Arabia

Reviewers

Name	Role	Comments	Date
Mohd Tehseen	Process Owner PNU IT		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	08/10/2012	First Draft – Created by Surjajyoti Chowdhury
1.0	04/10/2013	Baselined from the draft
1.1	10-07-2018	Removed logo and completed review
1.2	06-May-2020	Updated new Logo , Updated PNU management.

Referenced Documents

The following documents should be read in conjunction with this document:

Name	Version	Location

1 Introduction

The objective of this document is to detail out the guidelines to govern IT Service Continuity Management process. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the IT Service Continuity Management process in the organization

2 Scope

ITSCM covers:

- All services that are considered to be business critical irrespective of whether formal SLAs exist or not. These need to be captured in the plan

From process perspective, ITSCM process covers:

- Agreeing the scope of the ITSCM process
- Conducting Business Impact Analysis (BIA) to quantify the impact loss of IT service would have on the business.
- Identifying and assessing risks to identify potential threats to continuity and the likelihood of the threats becoming reality. Taking measures to manage the identified threats where this can be cost-justified. This follows the two steps identified above, and includes:
    - Elements of risk reduction
    - Selection of appropriate and comprehensive recovery options
- Preparing ITSCM plan and approaches that support business continuity requirements
- Testing of the plans
- Ongoing operation and maintenance of the plans

Out of Scope

1. Long-term risks such as those arising from changes in business itself i.e. direction, diversification, restructuring and so on, are out of the scope of ITSCM
2. Minor technical faults such as failure of components that do not have potential to have major impact on the business are out of scope of ITSCM. Such risks are managed and resolved through Incident Management process or planning that goes with processes of Availability Management, Problem Management, Change Management, Configuration Management

3 Policy Description

The policies for IT Service Continuity Management at PNU IT are as follows:

- An IT Service Continuity Management (ITSCM) process and Disaster Recovery Plan will be established and managed under a formal management process to help ensure quality and consistency across the organization.
- ITSCM Process scope covers all IT services which are essential for running of business process.
- Define, identify and roles and responsibilities for management of ITSCM process.
- Resources allocation on the basis of approved budget and business objective from ITSCM.
- Prepare Process Implementation Project Plan and Metrics before performing Requirement Analysis and Strategy definition activity.
- Identify Critical IT Services for business processes
- Critical It Services shall be assessed for risk and business impact to arrive at the service continuity plan.
- Continuity plan shall be developed by taking into account of agreed allowable downtime or degraded service levels in the event of any major loss of service.
- Continuity Plan shall be reviewed during any significant changes to IT Infrastructure or service.
- Roles and responsibilities and contact list in the service continuity management shall be defined, agreed and communicated.
- The Continuity Plan shall be tested no less frequently than once every two years and the results shall be analyzed which shall act as input to service improvement plan.
- Continuity Management shall ensure all service continuity documents are stored and maintained in a secure off-site location.
- Continuity Plan shall provide the staff with the understanding of their role in invoking and/ or executing the plans and the relevant access to the documents.

4 Acronyms

Acronym	Description
ECAB	ECAB Emergency Change Advisory Board
CSI	Continual Service Improvement
DC	Data Center
EUSS	End User Service Support
IT SMS	Information Technology Service Management System
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
KEDB	Known Error Database
NOC	Network Operations Center

OLA	Operational Level Agreement
PNU	Princess Noura Bint Abdulrahman University
RFC	Request for Change
CAB	CAB Change Advisory Board
ITSCM	IT Service Continuity Management

PNU IT

Problem Management Policy

Version: 1.3

Submitted to

Princess Nourah Bint Abdulrahman University

PNU, Saudi Arabia

Reviewers

Name	Role	Comments	Date
Rajeev Mookoni	Process Owner		
Ahsan Bashir	IT Infra Manager & Process Consultant		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJasser	PNU IT Operation Director		
SamiAwwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Sultanah AlJaser	PNU IT Operation Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	03/11/2011	First Draft – Created by Bhavesh Bijagare
1.0	20/02/2013	Baselined from draft version 0.1
1.1	27/04/2015	Changed approval matrix
1.2	12/07/2018	logo was removed from the document, annual review done on DATA
1.3	03/05/2020	PNU logo changed. Approver, reviewer, distribution list updated. “Wipro consulting” names removed

Referenced Documents

The following documents should be read in conjunction with this document:

Name	Version	Location

1 Introduction

The objective of this document is to detail out the guidelines to govern Problem Management process. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the Problem Management process in the organization

2 Scope

These principles will guide the process in execution from beginning to end through the organizational environment of infra and application support

Problem Management process in its current form will diagnose and rectify underlying causes of the symptoms (incident/(s)) in the IT infrastructure and application support environment to obtain the highest possible stability in IT service delivery.

Problem Management process in its current form will work proactively and reactively to perform Root Cause Analysis (RCA) of all issues through its delivery structure of various domains (e.g. Network, Storage, Backup, Database, Server, End User, Security, etc.)

3 Problem Management Process

Problem Management is the process responsible for managing the lifecycle of all reported problems. The primary objectives of Problem Management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented.

4 Process Governance Principles

The principles are designed to guide the operations of Problem Management and should be used to aid in the development of the PNU IT organization's Problem Management process and to deliver output as per the expectation

4.1 Acceptance to Corporate Policies & Regulatory Policies

- The Problem Management process shall adhere to IT service policies and shall be based on the needs of the business
- The Problem Management process shall adhere to existing security policies and procedures along with other regulatory requirements

4.2 Customer Focus

- The problem Management process shall in conjunction with PNU IT Management identify the business critical service areas and shall establish proactive monitoring on incident trends
- Problem Management shall direct its efforts to minimize the downtime by finding out the workarounds/solutions to the incidents within the agreed service levels, in a cost-justifiable way

4.3 Process Control

- The Problem Management process shall identify, record, classify and categorize the problem before initiating the root cause analysis.

Classification and categorization should mapped to incident classification and categorization

- The Problem Management process shall perform root cause analysis and trend analysis on the information collected from the Incident and Service Request Management database as well as other sources to identify potential preventive action
- The Problem Management process shall create workarounds and solutions plans based on risk assessments and shall work closely with other processes in its execution
- The Problem Management process shall own, maintain and manage the Known Error Database (KEDB). All known errors identified through root cause analysis shall be available in the KEDB. The KEDB shall be a single point of contact for all known errors. All up to date information should be provided to the incident and service request management process.
- The Problem Management process shall do process performance reporting

4.4 Establishing Problem Management in the organization

- **Establishing Roles and responsibilities**
  The Problem Management process shall define roles and responsibilities to manage the maintain (viz. problem recording, classification, diagnosis, solution and workaround creation and error management) the process and its relationship with other service management processes
- **Establishing Tools usage**
  Problem Management process shall identify tools to be used for problem recording till closure. Process shall also agree on the tools (e.g. KT, Fishbone etc.) used for performing RCA
- **Establishing Communication and Reporting**
  Problem Management shall have pre-defined communication channels for coordinating with cross functional groups, vendors, senior management and to handle escalation. Process also shall report all parameters as agreed with business
- **Establishing Skill Update structure**
  Problem Management process shall perform skill benchmarking of its entire staff to understand the knowledge and training requirement to run and manage the process. Process shall build skill update plan and report the progress against the plan
- **Establish Process Relationship**
  The Problem Management shall create a relationship map and relationship extent with all the service management process in scope
- **Escalation and Conflict Management**
  The Problem Management process shall have pre-defined escalation matrixes for all IT services. Process shall update and publish the details of these matrixes at appropriate intervals

4.5 Compliance Management

- The Problem Management process shall measure the compliance and also connect compliance findings to service improvements

- The Problem Management process shall follow organization wide audit and compliance process, if applicable

4.6 Process Review & Improvement

- Problem Management process shall review and validate the process regularly with all its stakeholders including tailoring requirements
- Problem Management process shall seek management review on principles of process governance
- Problem Management process shall provide all inputs to central process management function and process architecture unit for centralized process management

5 Acronyms

Acronym	Description
CMDB	Configuration Management Database
DC	Data Center
EUSS	End User Service Support
IT SMS	Information Technology Service Management System
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
KEDB	Known Error Database
NOC	Network Operations Center
OLA	Operational Level Agreement
PBM	Problem Management
PNU	Princess Noura Bint Abdulrahman University for Women
RFC	Request for Change
SLA	Service Level Agreement
UC	Underpinning Contract

PNU IT

Service Request Fulfillment Policy

Version: 1.2

PNU, Saudi Arabia

Reviewers

Name	Role	Comments	Date
Eyad GHA.Alshalabi	Process Owner		

Approvers

Name	Role	Signature	Date
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Operation Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Distribution

Name	Area	Name	Area
Ghadah Albugami	CIO		
Sultanah AlJaser	PNU IT Operation Director		
Sami Awwad Alnazi	Asst. IT Program Head		
Jehanzeb Rashid	Technical Advisor		

Document Control

Version	Date	Comments
0.1	03/11/2011	First Draft – Created by Bhavesh Bijagare
1.0	20/02/2013	Policy baselined from draft version 0.1
1.1	10-07-2018	Completed Annual Review and Removed Wipro Logo
1.2	06-May-2020	Updated PNU Logo and New PNU management.

Referenced Documents

The following documents should be read in conjunction with this document:

Name	Version	Location

1 Introduction

The objective of this document is to detail out the guidelines to govern Service Request Fulfillment process. The document is designed to make the PNU IT Team to get acquainted with the underlying process governance principles for the Service Request Fulfillment process in the organization

2 Scope

These principles will guide the process in execution from beginning to end through the organizational environment of infra and application support

Service Request Fulfillment process in its current form will identify and log any underlying Requests in the IT infrastructure and application support environment to obtain the highest possible stability in IT service delivery

Service Request Fulfillment process in its current form will work toward Categorization, Prioritization, Allocation, Resolution and Closure of the Requests

3 Service Request Fulfillment Process

Service Request Fulfillment is the process responsible for managing the lifecycle of all reported Requests. The primary objective of Service Request Fulfillment is to provide a consistent method for recording and tracking Requests until they are closed

4 Process Governance Principles

4.1 Acceptance to Corporate Policies & Regulatory Policies

- The Service Request Fulfillment process shall adhere to IT service policies and shall be based on the needs of the business
- The Service Request Fulfillment process shall adhere to existing security policies and procedures along with other regulatory requirements

4.2 Customer Focus

- Service Request Fulfillment shall direct its efforts to minimize the impact of Requests on the business by fulfilling service as quickly as possible within the agreed service levels, in a cost-justifiable way and meet Customer Expectations

4.3 Process Control

- The Service Request Fulfillment shall define procedures to handle Requests
- Service Request Fulfillment Process shall include
  - Recording
  - Allocation of priority
  - Classification
  - Updating of records
  - Escalation

  - Resolution
  - Closure
- The Service Request Fulfillment process shall do process performance reporting

4.4 Establishing Service Request Fulfillment in the organization

- **Establishing Roles and responsibilities**
  The Service Request Fulfillment process shall define roles and responsibilities to manage the maintain (viz. Request recording, classification, prioritization, allocation, resolution, closure and escalation) the process and its relationship with other service management processes
- **Establishing Tools usage**
  Service Request Fulfillment process shall identify tools to be used for Request recording till closure
- **Establishing Communication and Reporting**
  Service Request Fulfillment shall have pre-defined communication channels for coordinating with cross functional groups, vendors, senior management and to handle escalation
- **Establishing Skill Update structure**
  Service Request Fulfillment process shall perform skill benchmarking of its entire staff to understand the knowledge and training requirement to run and manage the process. Process shall build skill update plan and report the progress against the plan
- **Establish Process Relationship**
  The Service Request Fulfillment shall create a relationship map and relationship extent with all the service management process in scope
- **Escalation and Conflict Management**
  The Service Request Fulfillment process shall have pre-defined escalation matrixes for all IT services. Process shall update and publish the details of these matrixes at appropriate intervals

4.5 Compliance Management

- The Service Request Fulfillment process shall measure the compliance and also connect compliance findings to service improvements
- The Service Request Fulfillment process shall follow organization wide audit and compliance process, if applicable

4.6 Process Review & Improvement

- Service Request Fulfillment process shall review and validate the process regularly with all its stakeholders including tailoring requirements
- Service Request Fulfillment process shall seek management review on principles of process governance
- Service Request Fulfillment process shall provide all inputs to central process management function and process architecture unit for centralized process management

5 Acronyms

Acronym	Description
CMDB	Configuration Management Database
DC	Data Center
EUSS	End User Service Support
IT SMS	Information Technology Service Management System
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base
KEDB	Known Error Database
NOC	Network Operations Center
OLA	Operational Level Agreement
PNU	Princess Noura Bint Abdulrahman University for Women
RFC	Request for Change
SLA	Service Level Agreement
SRF	Service Request Fulfillment
UC	Underpinning Contract