Bahrain Polytechnic

Information and Communication Technology Services Policy

Document Information

- **Policy Title**: Information and Communication Technology Services
- **Version**: 4
- **Policy Reference**: C-IT-007
- **Effective Date**:
- **Last Reviewed**: 7 November 2023
- **Next Review Date:** 4 years cycle or when needed

Prepared By

- **Responsible Directorate**: **Information and Communication Technology Services**

Approved By

- **Executive Management Team (EMT)**
- **Approval Date**: [Date EMT Approval]

Bahrain Polytechnic Quality Management System

Policy Section: Corporate

Policy Title: Information and Communication Technology Services C-IT-007

Table of Contents

Policy: Information and Communication Technology Services C-IT-007

Policy Reference: C-IT-007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Policy Statement

Information Communication and Technology Services (ICTS) is committed to providing high-quality and sustainable services to support the Bahrain Polytechnic community. These services are in line with international standards and ensure reliable, effective, efficient, safe, and secure processes that will enable staff and students to fulfil Bahrain Polytechnic's vision and mission and enhance teaching and learning opportunities.

Application

People:

- Staff
- Students
- Other authorized individuals

Processes:

- ICT assets and services provision
- Maintenance and support
- Backup and restore.
- Data protection
- Network infrastructure management

External Requirements

This policy helps Bahrain Polytechnic meet the external requirements of the following bodies where applicable:

- Cabinet Affairs
- Central Informatics Organisation (CIO)
- E-Government

- Civil Service Bureau (CSB)
- Higher Education Council (HEC)
- Information Technology Infrastructure Library (ITIL)
- Ministry of Finance (MOF)

What is Expected:

- Enhancement of teaching and learning opportunities by effective use of ICT services.
- Maintenance and planning for effective ICT management systems and reporting mechanisms to ensure overall Bahrain Polytechnic efficiency.
- Maintenance of an effective communication process across Bahrain Polytechnic.
- Maintenance of ICT security, risk management, and data protection in a controlled environment.
- Maintain and Maintenance all software applications.
- Solve any Technical issues under the global standards with full documentation.
- Maintain all hardware and network.
- recommend the hardware/software needed for the other departments based on business requirements.
- Improvement Bahrain Polytechnic Security and Security Awareness Training.

Key Links and Related Documents

- Managing ICT Incidents Procedure
- Managing Corporate ICT Services Requests Procedure
- Managing Academic ICT Services Requests Procedure
- Course Management on the Learning Management System
- Managing ICT Business Applications
- Managing IT Corporate Resources
- Desktop Security Guideline
- Password Guideline
- Bring Your Own Device (BYOD) Guideline

Procedure: Managing ICT Incidents P-C-IT-007.001

Procedure Reference: P-C-IT-007.001
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure is to outline the steps to manage ICT incidents effectively and efficiently based on ITIL.

Related Policy

- Information and Communication Technology Services Policy C-IT-007

Related Documents (Rules, Guidelines, Flowcharts, Forms)

- Helpdesk Service Flowchart
- ICTS Guidelines

Procedures

General

- If the incident requires further clarification from the user and no response is received within a specified period (3 working days), the incident will be marked as closed. The user will be notified by email at the time of incident closure.
- When an incident is assigned to the ICT responsible team, the team is accountable for taking appropriate action to resolve the incident.
- If the ICT responsible team requires more information to proceed, they must contact the user through the incident or phone to gather the necessary details
- Incident Management, incidents are categorized based on their impact and urgency, which helps determine their priority and response as below:
  - **Normal Incident:** Normal incidents typically include issues that disrupt service but don't affect critical downtime or affect a large portion of the user. These can be handled in the normal procedure of operations.

- **Impact:** Limited to a specific service, system, user
- **Urgency:** It does not require immediate action

➢ **Major Incident:** Incident that causes significant disruption to critical business services or operations and affects many users or systems.

- **Impact:** High impact, affecting many users, critical systems or key services.
- **Urgency**: Then it is requiring immediate action

Incident Priority Matrix (SLA)

Urgency ↓ Impact →	Polytechnic Wide	Single/Multiple Department/Building OR more than 10 users	Individual
Work blocked	Critical	Critical	Moderate
Work degraded	High	High	Normal
Work not affected	Moderate	Moderate	Normal

Process to raise an incident

Some certain incidents may result in identifying a deeper issue that requires either:

- A **Change Request** (if it needs a system or configuration change),
- A **Problem** Record (if the root cause needs further investigation).

In such cases, the incident will be linked to the corresponding Change or Problem in the ICT Helpdesk, and users will be updated accordingly.

Step	Responsible	Outcome	Location (Optional)
1. Contact the ICTS helpdesk through Helpdesk System (Portal) to raise the incident, phone or walk-in to explain the incident	Affected User (Staff and Student)	Incident number	ICT Helpdesk portal ,phone or Building 9
2. Notify the affected user (Staff and Student) of the incident number	Helpdesk System (Automated)	Notification email	ICT Helpdesk portal

Step	Responsible	Outcome	Location (Optional)
3. Collect all relevant details **to Identify, categorize and prioritize Incidents based "incident SAL":** assessing the impact and urgency of incidents to determine how quickly to be handled and assigned to the responsible team.	Helpdesk Team	• *Assessment result(Normal/Major) • Notification email to user if the information/report required more clarification • IR assign to responsible team/ICT Helpdesk	ICT Helpdesk portal or phone
4. If the assessment result is "Normal"	• ICT Helpdesk 1st step • ICT Responsible team 2nd step, if required	• Resolve/Close the incident with comments	ICT Helpdesk portal
5. If the assessment result is "Major"	• ICT Helpdesk 1st step • ICT Responsible team 2nd step, when ICT Helpdesk couldn't resolve the issue	• ICT Helpdesk assess the issue and resolve it if they are possible. • Otherwise, the responsible team check the issue through the incident (contact user if required more information) • Send announcement (Planned/unplanned maintenance) notification email to all BP staff and student.	ICT Helpdesk portal or phone Email
6. Following step (5), once the ICT responsible team has resolved the major incident	ICT responsible team	• If the resolution of the incident results requires a change, the ICT responsible team must raise or update a	ICT Helpdesk portal

Step	Responsible	Outcome	Location (Optional)
		Change Request accordingly. • Change Request must include the following details: ○ Change Description ○ Reason for Change ○ Impact and Risk Assessment ○ Proposed Implementation Plan ○ Backout/Recovery Plan ○ User Acceptance Testing (UAT) ○ Approval and Authorization (to deploy the change) ○ Lessons Learned and Recommendations • Resolve/close the incident with comments and link to the change number.	
7. Following step (5), in cases where the ICT responsible team is unable to resolve the major incident:	Different Department or Vendor-Third party	• Escalate to: ○ Different Department ○ Vendor- Third party • If handled through escalation and the IR will be resolved ○ Resolve/close the incident with comments	ICT Helpdesk portal Email
8. If by escalation cannot resolve the issue	ICT responsible team	• Raise **Problem** and do more investigation	ICT Helpdesk portal

Step	Responsible	Outcome	Location (Optional)

		• The Problem must include the following details:
		  ○ Problem Description
		  ○ Root Cause
		  ○ Current Status
		  ○ Impact Assessment
		  ○ Workaround (if applicable)
		  ○ Resolution Plan / Permanent Fix (if known)
		  ○ Related Incident(s)
		  ○ Lessons Learned
		  ○ Recommendation / Preventive Action
		• Resolve
		• Close the incident with command	

*Assessment: by doing assessment clarifying the issue with user in details. ** Announcement email: If the incident is unresolved and is causing significant service impact, send the announcement.			

Procedure: Managing Academic ICTS Requests for New Academic Year P-C-IT-007.002

Procedure Reference: P-C-IT-007.002
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure is to manage academic service requests at the beginning of each new academic year in relation to ICTS assets; including software and hardware, efficiently and effectively.

Related Policy

- Information and Communication Technology Services Policy C-IT-007

Related Documents (Rules, Guidelines, Flowcharts, Forms)

- ICT Services Request through Helpdesk System
- New academic year Computer Labs preparation v1.0 – Flow Chart

Procedures

Step	Timeline*	Responsible	Outcome	Location (Optional)
1. *Complete the Request Form available on Helpdesk System.	February - April	Requester	Completed request	Helpdesk system
2. Notify the requestor with the ticket number		Helpdesk system (Automated)	Notification email	Helpdesk system
3. Obtain initial approval from the authorised management level.		Requester	Initial Approval	Helpdesk system

Step	Timeline*	Responsible	Outcome	Location (Optional)
4. Seek approval from the authorised management level and submit to ICT Helpdesk System		Requester	Received approval request	Helpdesk system
5. **Verify the request and complete it or assign it to the corresponding team		Helpdesk Team	Verified request	Helpdesk System
6. Assess the completed Request based on the following criteria: I. Compatibility and Availability with the existing infrastructure	End of May	ICTS Team	Recommendation on the appropriateness of the request decided	Helpdesk System
7. ***Notify the requestor of the request status and request a further level of approval if required.		ICTS Team	Requestor Notified	Helpdesk System
8. Process the approved request and procure if necessary (Refer to the Procurement Procedure)	June-Sep	ICTS Team	Request Processed	Helpdesk System
9. Deliver the requested ICT asset, software or hardware to the requestor in coordination with the fixed asset team and inventory	January	ICTS Team	Service Delivered	Helpdesk System
10. Provide feedback on the quality of services provided by ICTS		Requester	Feedback	Helpdesk System
11. Report to OMT the status of the services provided across the Polytechnic.		ICTS Team	Beginning of the Academic Semester	
*Faculty representatives must attend any meeting requested by ICTS before the end of May. Requestor non-compliance with the timeline may result in the delay or rejection of the request.				
**If the request is rejected the requestor will be notified by email. ***Update the requestor with the progress of the request until closed.				

Procedure: Managing ICT Corporate Services Requests P-C-IT-007.003

Procedure Reference: P-C-IT-007.003
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure is to manage service requests that relate to ICTS assets including corporate software and hardware efficiently and effectively.

Related Policy

- Information and Communication Technology Services Policy C-IT-007

Related Documents (Rules, Guidelines, Flowcharts, Forms)

- ICT Services Request through Helpdesk System

Procedures

Step	Responsible	Outcome	Location (Optional)
1. Complete the Request Form available on Helpdesk System.	Requester	Completed request with approval received	Helpdesk System
2. Notify the requestor with the ticket number	Helpdesk System (Automated)	Notification email	Helpdesk System
3. Obtain initial approval from the authorised management level.	Requestor	Initial Approval	Helpdesk system
4. Seek approval from the authorised management level and submit to ICT Helpdesk System	Requester	Received approval	

Step	Responsible	Outcome	Location (Optional)
5. *Verify the request and complete it or assign it to the corresponding team	Helpdesk Team	Verified request	Helpdesk System
6. Assess the completed Request based on the following criteria: Compatibility and availability with the existing system	ICTS Team	Recommendation on the appropriateness of the request	
7. **Notify the requestor of the request status and request a further level of approval as required.	ICTS Team	Requestor Notified	Helpdesk System
8. Process the approved request and procure if necessary (Refer to the Procurement Procedure)	ICTS Team	Request Processed	
9. Deliver the requested ICT access, asset, software or hardware to the requestor with the integration for fixed assets and inventory team	ICTS Team	Service Delivered	
10. Mark the request as complete	ICTS Team	Ticket closed	Helpdesk System
11. Provide feedback on the quality of services provided by ICTS	Requestor	Feedback	Helpdesk System
12. Report to OMT the status of the services provided across the Polytechnic.	ICTS Team	Beginning of the Academic Semester	
*If the request is rejected the requestor will be notified by email. **Update the requestor with the progress of the request until closed.			

Procedure: Course Management on the Learning Management System P-C-IT-007.004

Procedure Reference: P-C-IT-007.004
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure and the associated set of guidelines provide steps on the Learning Management System (LMS) at Bahrain Polytechnic.

Related Policy

- Information and Communication Technology Service Policy C-IT-007

Related Documents (Rules, Guidelines, Flowcharts, Forms)

- LMS Administration Guidelines and Roles (Available on Moodle)
- Academic Integrity and Honesty Policy A/AB/003
- Enrolment and Academic Progression Policy A/AB/018
- Programme Approval and Follow-up Policy A/AB/001

Procedure

Course Setup on LMS:

Step	Responsible	Outcome	Location (Optional)
1. ICT take the active courses list from Banner before a week of the semester starts to activate	ICTS Team	Existing courses activated and new courses created	Moodle

Step	Responsible	Outcome	Location (Optional)
the current courses in Moodle and to create new courses.			
2. *All Programme managers, Head of School and Dean of the related newly created course category will be enrolled automatically as ICT is maintaining their access on semester bases in Moodle category level (requesting this information from the academics' admins).	ICTS Team	Programme manager/ HOS and Dens enrolled In their categories	
*Should staff need a course set up during the semester, a service request needs to be raised with the approved course descriptor attached following the same procedure in (P-C-IT-007.003).			

Adding students to the LMS

Step	Responsible	Outcome	Location (Optional)
Moodle Banner integration is in place. ICT update the semester code in Banner view only to reflect the current running semester.	ICTS Team	All students enrolled in their registered courses	LMS courses

Adding Teaching Staff to Courses during the Semester

Step	Responsible	Outcome	Location (Optional)
1. *Send requests to the Programme Manager or Course Coordinator[1]	Course Coordinator		Individual Courses on the LMS
*Should the Programme Manager or Course Coordinator not know how this is done, see 'Requests' below.			

LMS Related Requests

Follow procedure in (P-C-IT-007.003)

Procedure: Managing ICT Business Applications P-C-IT-007.005

Procedure Reference: P-C-IT-007.005
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure is to outline the actions for managing ICT Business Applications from request to deployment on ICT infrastructure in an effective and efficient manner. The Business Applications include all applications that are vital to running Bahrain Polytechnic's business and can range from large line-of-business systems to specialised tools either on the user's computers or server including customised third-party systems, enterprise systems, and or internally developed systems, however, it does not include commercial off-the-shelf products.

Related Policy

- Information and Communication Technology Services Policy C-IT-007

Related Documents (Rules, Guidelines, Flowcharts, Forms)

- ICT Business Application Request Form
- ICTS Guidelines
- ICT Business Application Deployment Application Form
- Procurement Procedure

Procedures

Step	Responsible	Outcome	Location (Optional)
1. Complete the Request Form available on the Helpdesk System.	Requester	Completed request with approval received	Helpdesk System
2. Notify the requestor with the ticket number	Helpdesk System (Automated)	Notification email	Helpdesk System
3. Obtain initial approval from the authorized management level.	Requestor	Initial Approval	Helpdesk system
4. * Seek approval from the authorized management level and submit to ICT Helpdesk System	Requester	Received approval	Helpdesk system
5. Review the request and its attachment and notify the requestor of any missing information required for evaluation.	ICTS Team (One Week from receiving the full request application)	Request Reviewed	Helpdesk system
6. Evaluate the request based on defined Business Applications criteria in consultation with relevant stakeholders (refer to ICTS guidelines)	ICTS Team	Evaluation report	Helpdesk system
7. Notify the requestor of the request status, justification and alternative solution (if applicable).	ICTS Team	Requestor Notified	Helpdesk system
8. Purchase resources as per Procurement Procedure for new ICT BA.	Refer to Procurement Procedure	ICTS to be consulted for technical input	Helpdesk system
9. Create a change request ticket to proceed with the request	ICTS Team	Change request ticket created	Helpdesk system
10. Reserve the required resources for the ICT BA deployment/development and	As per resource availability	ICTS (vendor; if needed)	Helpdesk system

Step	Responsible	Outcome	Location (Optional)
start the work on the testing environment.			
11. Assign user acceptance testing (UAT) forms to the requestor and relevant end users for testing.	ICTS Team /Requestor/Stockholders	User Feedback	Helpdesk system
12. Take approval on the UAT form from the stakeholder – in case not approved repeat steps (10,11 and 12)	Stakeholder	Approved UAT	Helpdesk system
13. Take the required approval from ICT management to start on live environment	ICTS Team	Approved request to go live	Helpdesk system
14. If downtime is required, take approval from business owner and send announcement to relative end users.	ICTS Team and business owner	Announcement	Email
15. Reserve the required resources for the ICT BA deployment/development on the production environment (BA going live) in cooperation with the requestor	As per resource availability	Required request applied on live and ready to be used	Helpdesk System
16. Close the service ticket and the change request ticket	ICTS Team	Tickets closed	Helpdesk System
17. Provide feedback on the quality of services provided by ICTS	Requester	Feedback	Helpdesk System
18. Report to OMT the status of the services provided across the Polytechnic.	ICTS Team	Beginning of Academic semester	
*If the request is rejected the requestor will be notified by email.			

Procedure: Managing IT Corporate Resources P-C-IT-007.006

Procedure Reference: P-C-IT-007.006
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure is to manage IT assets under the custody of the Information and Communication Technology Services including corporate software and hardware in an efficient and effective manner.

Related Policy

- Information and Communication Technology Services Policy C/IT/006

Related Documents (Rules, Guidelines, Flowcharts, Forms)

- ICTS Request Form F/C-IT-007.001
- ICTS VPN Request Form
- ICTS Network Service Request Form
- Event ICTS Support Request Form
- ICTS Guidelines

Procedures

Step	Responsible	Outcome	Location (Optional)
1. Complete the Request Form available on Helpdesk System.	Requester	Completed request with approval received	Helpdesk System
2. Notify the requestor with the ticket number	Helpdesk System (Automated)	Notification email	Helpdesk System
3. Obtain initial approval from the authorised management level.	Requestor	Initial Approval	Helpdesk system
4. Seek approval from the authorised management level and submit to ICT Helpdesk System	Requester	Received approval	
5. *Verify the request and complete it or assign it to the corresponding team	Helpdesk Team	Verified request	Helpdesk System
6. Assess the completed Request based on the following criteria: Compatibility and availability with the existing system	ICTS Team	Recommendation on the appropriateness of the request	
7. **Notify the requestor with the request status and request a further level of approval as required.	ICTS Team	Requestor Notified	Helpdesk System
8. Process the approved request and procure if necessary (Refer to the Procurement Procedure)	ICTS Team	Request Processed	Helpdesk System

Step	Responsible	Outcome	Location (Optional)
9. Deliver the requested ICT asset, software or hardware to the requestor with the integration for fixed assets and inventory team	ICTS Team	Service Delivered	Helpdesk System
10. Provide feedback on the quality of services provided by ICTS	Requestor	Feedback	Helpdesk System
11. Report to OMT the status of the services provided across the Polytechnic.	ICTS Team	Beginning of Academic semester	
*If the request is rejected the requestor will be notified by email. **Update the requestor with the progress of the request until closed. Note: ICT has the right to monitor all IT assets and to reset any configuration or set up different than what ICTS has configured.			

Procedure: Student Account Request P-C-IT-007.007

Procedure Reference: P-C-IT-007.007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure is to manage service requests for all Regular students, Con-Ed students, Top up students, and Acceleration students in relation to ICTS resources such as but not limited to creating user ids (e.g.: Active Directory, Banner, and Moodle, etc) for students, in an efficient and effective manner.

Related Policy

- Information and Communication Technology Services Policy C-IT-007

Related Documents (Rules, Guidelines, Flowcharts, Forms)

- ICT Services Request through Helpdesk System
- ICTS Guidelines

Procedures

Step	Responsible	Outcome	Location (Optional)
1. *Complete the Service Request Form available on the Helpdesk System.	Requester (Admission/Registration Department)	Completed request	Helpdesk system

Step	Responsible	Outcome	Location (Optional)
2. Notify the requestor with the ticket number	Helpdesk system (Automated)	Notification email	Helpdesk system
3. Obtain initial approval from the authorized management level.	Requester (Admission/Registration Director)	Initial Approval	Helpdesk system
4. Seek approval from the authorized management level and submit to ICT Helpdesk System	Requester (Admission/Registration Director)	Received approval request	Helpdesk system
5. **Verify the request and complete it or assign it to the corresponding team	Helpdesk Team	Verified request	Helpdesk System
6. Assess the completed Request based on the following criteria: II. Compatibility and Availability with the existing infrastructure	ICTS Team	Recommendation on the appropriateness of the request decided	Helpdesk System
7. ***Notify the requestor with the request status and request a further level of approval if required.	ICTS Team	Requestor Notified	Helpdesk System
8. Process the approved request and procure if necessary (Refer to the Procurement Procedure)	ICTS Team	Request Processed	Helpdesk System

Step	Responsible	Outcome	Location (Optional)
9. Deliver the requested ICT resource as here is the student user ids	ICTS Team	Service Delivered	Helpdesk System
10. Provide feedback on the quality of services provided by ICTS	Requester	Feedback	Helpdesk System
11. Report OMT (Operation Management team) the status of the services provided across the Polytechnic.	ICTS Team	Beginning of Academic Semester	

Procedure: Request for Replacing Hardware P-C-IT-007.008

Procedure Reference: P-C-IT-007.008
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this procedure is to outline the actions required while Bahrain Polytechnic's staff required to replace the hardware such as laptop, PC, etc.

Related Policy

Information and Communication Technology Services Policy C-IT-007

Related Documents (Rules, Guidelines, Flowcharts, Forms)

ICT Services Request through Helpdesk System/ portal

Procedure

General

At Bahrain Polytechnic, employees receive computing devices (laptop or desktop) according to the following guidelines:

- **Standard Allocation**: Each employee is typically allocated one device, either a laptop or desktop.
- **Exceptions**: With appropriate justification and management approval, an employee may be allocated two devices (e.g., one laptop and one desktop).

This procedure ensures staff members have access to the necessary equipment while maintaining proper controls through a justification and approval process.

Processes to receive/replace devices

Step	Responsible	Outcome	Location (Optional)
1. Raise the Service Request (SR) Form via ICT Helpdesk System.	Requestor	Completed request with approval received	ICT Help Desk portal
2. Notify the requestor with the ticket number	Helpdesk System (Automated)	Notification email	ICT Help Desk portal
3. Obtain initial approval from the authorised management level.	Requestor's Manager	Initial Approval	ICT Help Desk portal
4. *Assess the request to take proper action	ICT Technician	Evaluate the request	ICT Help Desk portal
5. ** Based on point No. 4, when "Rejected by ICT Technician," the requester will receive a rejection notification along with the justification. The rejection justification such as but not limited to: • Under ****Warranty (the device is still in service). • Hardware is physically damaged-it is under warranty (escalate the issue to **HR and Finance** for further action). • The required hardware is not available in stock, ICT Technician will notify user when replacement hardware becomes available.	ICT Technician	Reject the request	ICT Help Desk portal
6. Based on point No. 4, once Approved by the ICT Technician, a request will be sent to the "Stores" team to check if the requester has any other items under their custody, and the email will be attached.	ICT Technician	Check what is under the requester's custody	Email
7. Upon receiving a "Yes" from the store, the next steps will be carried out accordingly • ICT Technician to provide the "Technical Report including these	ICT Technician	• ICT Technical Report (A detailed description of the replacement hardware)	ICT Help Desk portal

Step	Responsible	Outcome	Location (Optional)
items" – this report is to return the old hardware. • ***Also to provide "Store Transfer Form"- this form approval from ICT to receive new Hardware, the form filled with hardware/device description model. Requester to be notified via helpdesk portal to pass by ICT helpdesk office to collect the approved form/report.		• Store Transfer Form(approval from ICT technician).	
8. Upon receiving a "No" from the store, the ICT Technician will provide the "Store Transfer Form" along with the hardware/device description and model. Requester to be notified via helpdesk portal to pass by ICT helpdesk office to collect the approved form.	ICT Technician	Store Transfer Form(Approval from ICT technician)	ICT Help Desk portal
9. The request to be closed with this comment "Approval form has been submitted to the user to receive the requested item from the stores team"	ICT Technician	Request is fulfilled Close the request with comments	ICT Help Desk portal
*ICT Technician to perform a technical assessment (is the replacement justifiable based on the requirement, hardware model, specs and age). ** The ICT technician team rejects the request if the replacement device/hardware doesn't have a reasonable justification. *** a notification for the store team that this form is not to be processed before the user returns the items in the technical report. ****Warranty specification based on this document(Page 287) from Ministry of Finance and National Economy			

Guidelines: Desktop Security

Policy Reference: Information and Communication Technology Services C/IT/007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The Purpose of this guideline is to provide the most secure work environment that is suitable for Bahrain Polytechnic staff and students and consider the needs of an educational institution, while reducing the risks to the enterprise's information and IT systems.

Scope

This guideline applies to all Bahrain Polytechnic Users (Staff and/or Students) of information and communication technology (ICT) resources that is owned, managed by Bahrain Polytechnic.

Individual/personnel covered in these guidelines are all Bahrain Polytechnic Users of students, alumni, employees (full or part-time), contractors, consultants and all personnel affiliated with third parties in accompanying business with the Polytechnic.

ICT resources covered in this guideline cover all desktops/laptops/tablets (machines)that is owned by Bahrain Polytechnic.

Guideline Statement

General Information

- ICT resources are provided for legitimate Bahrain Polytechnic activities, and all usage must be consistent with this purpose and the Bahrain Polytechnic Users must ensure that they are kept securely when not in use, or while being transported and returned when they leave Bahrain Polytechnic.
- Bahrain Polytechnic Users should ensure they are efficient and professional in their use of ICTS network facilities (Desktop/Laptop), services and applications.
- Bahrain Polytechnic Users are responsible for keeping their account information secure and not share with others.
- Bahrain Polytechnic Users of Bahrain Polytechnic's information systems will be responsible and liable for all actions including transactions, information retrieval or communication performed on their devices by using their User ID(s) and password(s) this is include responsibility for using machines inside and outside (any public place or during business trip) of Bahrain Polytechnic.
- Upgrading Operation System (OS)/ and Application (services) patching is a must to prevent any threats/attacks; Bahrain Polytechnic Users must accept ICTS team for implementing the upgrades and patching, otherwise they are responsible in case of any security breach.
- Bahrain Polytechnic Users not allowed amending their desktop/laptop/tablet configuration (such as but not limited to: security settings for Active Desktop, Computer, Control Panel, Explorer, Internet Explorer, Network, System categories, etc.) unless authorized on request.
- Bahrain Polytechnic does not allow to install pirated software copy on Bahrain Polytechnic machines.
- If requester/user makes an infringing copy of Bahrain Polytechnic software with the aim of procurement a commercial advantage or profit, this will take as a criminal offence.
- Bahrain Polytechnic required that Bahrain Polytechnic Users use and install software in compliance with licence terms and conditions.
- For security purpose user will not granted local admin privileges in all cases to secure the environment, such requirement need to be through ICTS Helpdesk Portal, alternately Bahrain Polytechnic Users can use Software Centre for install an uninstall software.
- Bahrain Polytechnic Users should not accesses or uses electronic communication resources that is not under his authorized IDs in a way that is not authorized.

Bahrain Polytechnic Minimum Standard

- All machines owned or leased by Bahrain Polytechnic must be joined to the local work domain.

Visitor/Contractor/Consultant Machines

- Non-Bahrain Polytechnic machines for Visitor/Contractor/Consultant is not authorized to use Bahrain Polytechnic's network or alternatively they can use Bahrain Polytechnic lease machine or public wireless.
- Visitors, contractors, consultants and third party need to be informed of the Bahrain Polytechnic standard before they arrive to ensure that a proper tool in place, or be willing to allow ICTS staff to install the required tools.

Implement strong password syntax and protect your password

The key for complete access to your computer is your password. There are countless programs that attempt to determine passwords. The best defence is a strong password. This makes the password nearly impossible to guess in a reasonable amount of time.

For strong password

- Don't use any names, be it a relative of yours or a character in a novel, book, or movie.
- Don't share your password/application-specific account details with anyone.
- Don't use "remember my password feature".
- Passwords should not be based on any of the following:
    - Months of the year, days of the week or any other aspect of the
    - Date (like date of birth, date of joining, anniversary, etc);
        - Family names or initials;
        - Vehicle registration numbers;
        - Employee No. / Employee D or designations;
        - Project or department name or references;
        - Company names, identifiers or references;
        - Telephone numbers or similar all-numeric groups;
        - User lD, user name, group lD or other system identifier;
        - More than two consecutive identical characters;
        - All numeric or all-alphabetic groups; or
        - Any standard dictionary word (without incorporating special
        - characters, mixed case, and other elements).

Password Guidelines

- Password must meet complexity requirements
- Password should not contain the user's account name or parts of the user's full name that exceed two consecutive characters

- Password must be at least eight characters in length
- Password must 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.
- User cannot use the current or the two previous passwords

Logout of finished sessions and lock the computer when left unattended

- Regardless of how the user is authenticated, there should be a mechanism for locking the account after 3-10 successive failures.
- Users must log out from or lock their Desktop/Laptop every time they leave their machines this is to prevent unauthorized access.

Physically secure your machine

- Never assume any location is completely secured, even if the location is restricted via swipe access or a locked door.
- Users must not move to a new location ICTS equipment that is ordinarily fixed (e.g. PC base units, printers, and monitors).

Protect confidential and sensitive information

- Bahrain Polytechnic Users need to use encryption software to protect confidential and sensitive information/data (Definition of confidential data as per Bahrain Polytechnic) stored in their machine or ask ICTS Helpdesk for help to do encryption.
- Bahrain Polytechnic Users should never send confidential and/or sensitive information via email. If they must send such information via email, encrypt the information before sending it.
- If Bahrain Polytechnic Users uses portable devices to store confidential and sensitive data, keep them physically secured and encrypt the confidential and sensitive information and data on them.
- Bahrain Polytechnic provides a different mechanism (SharePoint/One drive) of business da, therefore Bahrain Polytechnic Users must always use these machines to store work-related data and Bahrain Polytechnic Users is responsible for any data on their machine.

Scan email attachments before opening

- Opening e-mails with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, that she/he thinks may contain virus, instead, Bahrain Polytechnic Users should call ICTS Helpdesk and/or log an incident.
- Be cautious about clicking on links sent to you in email, it is very easy to create a link that hides the true location of where the link goes.

Monitoring

- Access rights of employees will be reviewed periodically to ensure that the access rights (physical or logical) granted to an employee corroborate with his/her roles and responsibilities. Access rights (physical or logical) deemed inappropriate will be revoked immediately. The periodicity will be as follows:
  - User privileges and system profiles reviewed annually
  - Unused, redundant, expired accounts reviewed quarterly
  - Privileged accounts (e.g., administrators) reviewed quarterly
- Changes resulting from the review of the access rights will be reported and acted through the ICTS Helpdesk.

Monitoring User of Internet

- The Internet connection will be adequately audited and monitored on a periodic basis to detect any unauthorized activity.
- At any time and without prior notice, the Bahrain Polytechnic reserves the right to examine and monitor the internet surfing activities.
- The Bahrain Polytechnic Users, visitors, contractors, consultants and third parties shall be responsible of notifying the ICTS Helpdesk immediately of any suspicious network activity or any security violation related to the Internet connection.

Virus and Malware Protection

- All machines that owned by Bahrain Polytechnic must run ICTS authorized licenses software including antivirus software.
- Any infected system will be isolated from the network infrastructure, quarantined, cleaned and disinfected to detect any other cases of infection.

- Prevent Bahrain Polytechnic Users from changing the configuration of removing, de-activation or otherwise tampering with any anti-malware software deployed on the various ICTS infrastructure.

Access to Wireless Networks

- Bahrain Polytechnic will have multiple wireless networks operating in the Campus to ensure segregation of access. Bahrain Polytechnic will segregate the users accessing the wireless services into three groups:
  - Polytechnic Staff
  - Polytechnic WiFi
- In any case of using VPNs or proxy altering hardware or software, the Wi-Fi access will be revoked immediately by the ICTS Security Team and registered as a threat to Bahrain Polytechnic's framework against the respective user.

Unethical and Unacceptable Behavior

- Bahrain Polytechnic Users is not allowed to amend their desktop/laptop/tablet configuration (such as but not limited to: security settings for Active Desktop, Computer, Control Panel, Explorer, Internet Explorer, Network, System categories, etc.) unless authorized on request.
- Bahrain Polytechnic does not allow to install of pirated software copies on Bahrain Polytechnic machines.
- For security purposes Bahrain Polytechnic Users will not grant local admin privileges in all cases to secure the environment, such requirements need to be through ICT Helpdesk Portal, alternately Bahrain Polytechnic Users can use Software Centre to install an uninstall software.
- Bahrain Polytechnic Users should not access or uses electronic communication resources that is not under his authorized IDs in a way that is not authorized.
- Uses the electronic communication resources without authorization to engage in spamming activities or invade the privacy of others
- Uses electronic communication resources without authorization to engage in mass communication within or outside the Polytechnic
- Creates a situation that results in inefficient or wasteful use of electronic communication resources
- Uses the electronic communication resource without authorization for personal gain
- Eating and drinking in the Classrooms & Computer Labs The Bahrain Polytechnic regulations prohibit eating and drinking, other than water, in classrooms, computers labs or drop-in-computer suites.
- When using USB devices, Bahrain Polytechnic users must use official devices and allow antivirus scans to complete before opening any files.

- Bahrain Polytechnic users are not allowed to bypass or disabling antivirus scan.
- USBs should be treated as temporary transfer tools and not for long term storage or backup of work-related data.
- Bahrain Polytechnic users are responsible for ensuring their devices are clean and do not contain harmful or unauthorized content.

Guidelines: Password Security

Policy Reference: Information and Communication Technology Services C/IT/007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The objective of this document is to set the requirements for the certain management of passwords used to access systems/services within Bahrain Polytechnic and to ensure such passwords are afforded acceptable levels of protection.

Scope

This guideline applies to all Bahrain Polytechnic employees, contracted personnel, and any third parties' representatives who have been provided access to information systems and applications of Bahrain Polytechnic. This guideline also applies to all systems and applications.

All passwords for applicable technical resources shall comply with the requirements of this guideline.

Guideline Statement

Password Management

- Passwords, regardless of which technical resource they grant access to, must be classified as top-secret, and must therefore not be disclosed to any other person.
- HR must provide the staff's details (Name, CPR, Staff ID, and Job title) before the creation of new accounts and passwords. Furthermore, these details must be entered into the appropriate fields within the applicable user object or directory service (Active Directory).
- Admission/Registration must provide the student's details (Name, CPR, Student ID) before the creation of new accounts and passwords. Furthermore, these details must be entered into the appropriate fields within the applicable user object or directory service (Active Directory).
- Users must use only their own user ID(s) and password(s) to access Bahrain Polytechnic resources unless it is technically not feasible to do so.
- Users will be held accountable and liable for all actions performed using their assigned user ID (s) and password(s).

Password Confidentiality

- User passwords shall always remain confidential and don't share your password/application-specific account details with anyone.
- Passwords must be entered in non-display fields (i.e. hidden by asterisks or similar graphical representation).
- Don't use any names, be it a relative of yours or a character in a novel, book, or movie.
- Don’t use the "remember my password feature".

Password Composition & Expiry

- Domain User Password Requirements:
- Password must meet complexity requirements
- Maximum password age is 90 days for both student and staff
- Password should not contain the user’s account name or parts of the user’s full name that exceed two consecutive characters
- Password must be at least eight characters in length
- Password must 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.
- User cannot use the current or the two previous passwords.

Password Reset

- Bahrain Polytechnic users cannot reset password through Multi-Factor Authentication (MFA), and technical support is needed in case user delete MFA application or format his/her mobile device.

- Bahrain Polytechnic users can reset their password reset password independently while MFA is active by using the provided password reset link. This process does not require the presence of technical support.
- Technical support will not reset staff and student's passwords without their presence.
- Once the user resets his/her own password, the account will be unlocked.

Authentication

- The User ID and password must be authenticated as a whole. Authentication failure must provide an error message to the user that does not indicate which element of the login credentials is incorrect (e.g. "incorrect login" and not "incorrect password" or "username does not exist").

Inactivity Lock

- The inactivity lock period (10 minutes) applies both to normal and super user accounts.

Password Selection Rules

- Users are encouraged to create passwords that are not easy to guess yet easy to remember by the respective user.
- Passwords should not be based on any of the following:
  - Months of the year, days of the week or any other aspect of the
  - Date (like date of birth, date of joining, anniversary, etc);
  - Family names or initials;
  - Vehicle registration numbers;
  - Employee No. / Employee D or designations;
  - Project or department name or references;
  - Company names, identifiers or references;
  - Telephone numbers or similar all-numeric groups;
  - User lD, user name. group lD or other system identifier;
  - More than two consecutive identical characters;
  - All numeric or all-alphabetic groups; or
  - Any standard dictionary word (without incorporating special characters, mixed case, and other elements).

Guidelines: Bring Your Own Device (BYOD)

Policy Reference: Information and Communication Technology Services C/IT/007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

To protect information stored on, processed by, or accessible via user endpoint devices against risks introduced by using these devices, in accordance with ISO 27002:2022 Control A.8.1. This Guideline establishes security requirements for personally owned devices (BYOD) that used for work-related purposes.

This guideline outlines the requirements for devices that need to connect to wired and wireless networks within the Bahrain Polytechnic domain.

Scope

This guideline applies to:

- Bahrain Polytechnic wired/wireless networks
- All Bahrain Polytechnic contractors, consultants, and authorized third parties
- Bahrain Polytechnic provides designated devices to employees for work-related purposes
- All user endpoint devices including but not limited to:
  - **Personal devices (BYOD):** Smartphones, tablets, laptops, smartwatches, and other personally owned computing devices

Guideline Statement

General Information

Bahrain Polytechnic recognizes that user endpoint devices are essential for productivity but introduce significant security risks. All endpoint devices accessing institutional information must comply with this policy to ensure adequate protection against information security threats.

Device Registration and Authorization

Personal Device Registration (BYOD)

- **Written Authorization:** Employees/Third party who need to use their personal devices for work purposes at Bahrain Polytechnic must submit a Service Request through the ICT Helpdesk. This request must include proper justification and be approved by their Manager/Director prior to use.
- **Security Assessment:** ICT will conduct a security assessment of the device compatibility and configuration
- **Signed Agreement:** Users must sign confidentiality agreement (User Acceptance) form for BYOD User Agreement acknowledging responsibilities and risks

Physical Security Requirements

Below protection in line with Cybersecurity/Desktop Security Guidelines

Device Protection – Under user responsibility

- **Physical Custody:** Users are responsible for maintaining physical custody of their endpoint devices
- **Secure Storage:** Devices must be secured when unattended (locked drawers, secure facilities)
- **Public Area Usage:** Extra care must be taken when using devices containing sensitive information in public or insecure areas
- **Loss/Theft Reporting:** Immediate reporting to Bahrain Polytechnic Security team

Environmental Protection – Under user responsibility

- **Environmental Hazards:** Protect devices from environmental threats (water, extreme temperatures, physical damage)
- **Transportation:** Use appropriate protective cases when transporting devices

Technical Security Requirements

Authentication and Access Control

- **Strong Authentication:** Employees and third parties who use their own devices for work must implement strong authentication measures, including:
    - Minimum 8-character passwords/PINs with complexity requirements

  - Multi-factor authentication for accessing corporate applications
- **Automatic Lock:** Devices must automatically lock after maximum 5 minutes of inactivity
- **Failed Attempt Protection:** Account lockout after 5 consecutive failed authentication attempts

Malware Protection

- **Antivirus Software:** Install and maintain current antivirus/anti-malware software with real-time protection (Antivirus should be up to date)
- **Regular Scanning:** Perform regular system scans and updates
- **Suspicious Activity:** Report any suspected malware or security incidents immediately

Data Classification and Handling

Permitted Data Types

Personal devices may access only the following types of institutional information:

- General business communications and approved email
- Non-sensitive documents and presentations
- Approved business applications and collaboration tools
- Public information and marketing materials

Prohibited Data Types

The following information types are strictly prohibited on personal devices:

- Information classified as CONFIDENTIAL, SECRET, or TOP SECRET per Bahrain Government regulations
- Student academic records and personal information
- Employee personal and HR information
- Financial records and sensitive business data
- Examination materials, answer keys, and assessment content
- Research data and intellectual property
- Large datasets exceeding 1 GB aggregate storage

Data Segregation

- **Separate Containers:** Corporate and personal data must be stored in clearly separated containers/directories
- **Clear Labeling:** Directories must be clearly labeled (e.g., "Personal" and "Work")
- **Application Segregation:** Use separate applications for personal and business purposes where possible

Examination and Restricted Environment Controls

Examination Environments – in link to Academic Policy/process

- **Complete Prohibition:** All personal mobile devices strictly prohibited in examination rooms and secure testing areas by responsible
- **Secure Storage:** Devices must be powered off and stored in designated secure areas during examinations
- **Staff Devices:** Only pre-approved institute devices permitted for examination staff, limited to essential functions

Secure Areas

- **Restricted Zones:** Additional restrictions apply in server rooms, data centers, and other secure facilities

User Responsibilities and Behavior

General Responsibilities

- **Policy Compliance:** Maintain compliance with all technical and procedural requirements
- **Security Awareness:** Participate in mandatory security awareness training
- **Incident Reporting:** Report security incidents, suspicious activities, or policy violations immediately
- **Software Licensing:** Ensure all software is properly licensed and legally obtained

Prohibited Activities

- **Unauthorized Access:** Attempting to access systems or data beyond authorized scope
- **Malicious Software:** Installing or executing malicious software or suspicious applications
- **Data Sharing:** Sharing corporate credentials or unauthorized data transfer
- **Policy Circumvention:** Attempting to bypass or disable security controls

Institutional Rights and Controls

Data and Device Management Rights

Bahrain Polytechnic reserves the right to:

- **Remote Access:** Access, backup, retrieve, modify, or delete corporate data on any registered device
- **Device Inspection:** Forensically examine devices containing or suspected of containing corporate data
- **Remote Wipe:** Remotely wipe corporate data or entire device if compromised, lost, or upon employment termination
- **Compliance Monitoring:** Audit device compliance with security policies through technical controls
- **Access Revocation:** Immediately suspend or revoke device access during security incidents

Privacy Considerations

- **Personal Data Protection:** Reasonable efforts to avoid accessing personal data during support or investigation
- **Notification:** Prior notification of planned access activities where operationally feasible
- **Audit Logging:** Maintenance of audit logs for all corporate data access activities

Incident Response and Reporting

Immediate Response Requirements

- **Lost/Stolen Devices:** Report immediately to Bahrain Polytechnic Security team
- **Security Incidents:** Report suspected malware, unauthorized access, or data breaches through ICT Helpdesk/ICT Security team
- **Technical Issues:** Report device malfunctions affecting security controls through ICT Helpdesk/ICT Security team

Response Procedures

- **Device Location:** Attempt remote device location and recovery
- **Remote Wipe:** Initiate remote data wipe if device cannot be recovered
- **Password Reset:** Reset all accounts accessible from compromised device, disabling main account
- **Investigation:** Conduct forensic analysis and impact assessment as required

Support and Maintenance

Technical Support

- **Institute Devices:** Full technical support through ICT Helpdesk

- **Personal Devices:** Limited support on "best efforts" basis for business applications only
- **Self-Service Resources:** Online documentation and troubleshooting guides available

Maintenance Requirements

- **Regular Updates:** Maintain current operating system and application versions
- **Compliance Monitoring:** Quarterly compliance verification and reporting
- **Performance Review:** Annual review of device performance and security posture

Employment Termination and Device Separation

Employee Departure – ICT Service Request required

- **Institute Devices:** Immediate return of all institute-provided devices and accessories
- **Personal Devices:** Mandatory corporate data transfer/backup based on manager request
- **Account Deactivation:** Immediate deactivation of all corporate accounts and certificates
- **Compliance Verification:** Confirmation of data deletion

Data Retention and Disposal

- **Corporate Data Backup:** Automated backup of corporate data prior to device separation
- **Secure Data Destruction:** Destruction of corporate data using approved methods
- **Compliance Documentation:** Maintenance of records demonstrating proper data disposal, it links to system log

Compliance and Monitoring

Compliance Monitoring

- **Regular Audits:** Quarterly compliance assessments and device inventory
- **Vulnerability Scanning:** Regular security scanning and penetration testing
- **Compliance Reporting:** Monthly compliance reports to management

Non-Compliance and Enforcement - in line with Human Resource Policy

- **Violation Categories:**
    - Minor: Additional training and verbal warning
    - Moderate: Written warning and temporary access restriction
    - Major: Suspension of device privileges and formal disciplinary action

- Severe: Employment termination and potential legal action

Training and Awareness

Mandatory Training

- **Initial Training:** Comprehensive security awareness training for all device users
- **Annual Refresher:** Yearly security update training and policy review
- **Role-Specific Training:** Additional training for users with elevated access or sensitive data
- **Incident Response Training:** Training on proper incident reporting and response procedures

Ongoing Awareness

- **Security Bulletins:** Regular communication of new threats and vulnerabilities
- **Policy Updates:** Notification of policy changes and updates
- **Best Practice Sharing:** Distribution of security tips and best practices

Guidelines: Cybersecurity

Policy Reference: Information and Communication Technology Services C/IT/007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The Purpose of this guideline is to provide the most secure work environment that is suitable for Bahrain Polytechnic staff and students and consider the needs of an educational institution while reducing the risks to the enterprise's information and IT systems.

Scope

- To ensure that all the Bahrain Polytechnic users (staffs and students) are aware of the professional, lawful and ethical use of the enterprise's information systems.
- Establish and maintain a standard, formal and continuous approach for the management of the information systems, enabling secure technology and business processes that are aligned with business requirements and enterprise security management of Bahrain Polytechnic.
- To ensure that the users are aware of their responsibilities and educated towards the fair usage of the ICT systems, assets, enterprise and personal information.
- To ensure that the all the affiliated terms and policies are carried out in the right disciplines.
- To ensure that the users are aware of when, where, and why monitoring may take place.
- Establish a process to ensure that the productive and efficient usage of ICT systems is being carried out on a granular level in the Bahrain Polytechnic.

Guideline Statement

- **General Information**
  - Bahrain Polytechnic considers its information resources (i.e., information maintained in any form and systems that process, store, or transmit such information) as assets. The need to secure its Information Assets becomes increasingly important for a successful transition between manual and automated systems should ensure data confidentiality, integrity and availability which require clear segregation of duties, defined information asset owners and defined roles and responsibilities.
  - ICT users are defined as individuals, departments, students, and vendors requiring ICTS services. The ICTS Users can be classified into the following:
    - Internal Users (Corporate and Academic): Bahrain Polytechnic Internal Departments to whom the ICT Department provides Services.
    - External Users: Students form the largest body of external users for Bahrain Polytechnic. Other than students, vendors will also be considered external users if they require access to the ICTS systems.
  - This guideline documents the responsibilities of all ICT users. Any user found to have violated this guideline may be subject to disciplinary action, up to and including termination of employment.
- **General Use and Ownership**
  - Users should be aware that the data they create on Bahrain Polytechnic's systems remains the property of Bahrain Polytechnic.
  - This information is not confidential and at any time, with or without notice, this information will be monitored, searched, reviewed, disclosed, or intercepted by Management/Human Resources for any legitimate purpose.
  - All Users of Bahrain Polytechnic's information systems will be responsible and liable for all actions including transactions, information retrieval or communication performed on Bahrain Polytechnic's information systems by using their User ID(s) and password(s).
  - Information Owners are generally Systems' business Owners (i.e: Banner Business Owners are Directors of Registery and Finance), and directors who are responsible for using the information for running and controlling the business. Information ownership refers to the allocation and assignment of responsibility to protect computer information, establish accountability and ensure that information is kept complete, confidential and accurate.
  - Sensitive information may not be removed from Bahrain Polytechnic premises unless there has been prior approval from the Information Owners.
  - Confidential information must only be disclosed after the Information Owner's explicit authorization has been obtained. If an individual has been granted access to confidential information, this does not imply the authority to disclose it to other persons.

- Systems' Business Owner/Human Resources reserves the right to revoke the privileges of any User at any time. Conduct that interferes with the normal and proper operation of Bahrain Polytechnic information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

➢ **System**

- Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Bahrain Polytechnic are prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses) are prohibited.
- Using Bahrain Polytechnic computing assets to actively engage in procuring or transmitting material that is in violation of generally accepted sexual harassment or hostile workplace policies are prohibited.
- Making fraudulent offers of products, items, or services originating from any Bahrain Polytechnic account are prohibited.

➢ **Respect for other User's Computing Resources**

- Users are given access to Bahrain Polytechnic's computing systems and network because they are tools to help you meet your business goals. This access, however, is a privilege, not a right. Preventing others from fulfilling their business-related goals by using the system irresponsibly is not permitted and will result in disciplinary action.
- Users agree not to obstruct other's work by using unnecessarily large amounts of system resources (such as disk space, output devices, CPU time, and network bandwidth) or deliberately causing any machine to crash or shut down. Being aware of the finite capacity of systems, Users agree to limit your own use so as not to interfere unreasonably with the activity of other Users. If it is determined that you are using excessive systems resources, your activity will be blocked or halted by the network administration staff.
- Users agree not to use someone else's account, either with or without permission. Individual accounts cannot be transferred to or used by another individual. Users also agree that attempts to gain access to any account not belonging to you or to a system on which you are not an authorized User will be treated as a violation of the User Obligation and will result in disciplinary action ranging from revocation of computing privileges to dismissal.

➢ **User Identification**

Each User is responsible for the login name or User-ID assigned to him/her and is accountable for the usage, access privilege and for any type of violations committed by their own User ID.

User-IDs may not be utilized by anyone but the individual to whom they have been issued. Users must not allow others to perform any activity with their User-IDs. Similarly, Users are forbidden from performing any activity with IDs belonging to other Users.
For the issue of a new login name, the defined processes will be followed by all the parties involved.
Official requests from Human Resource or System's Business Owner, either in hardcopy or as part of the internal workflow software like ICT Helpdesk System and/or email, should be submitted to ICT with appropriate approval.
Whenever employment is terminated (for any reason) for an employee with knowledge of such passwords, the affected passwords must be changed immediately. Also, Disable and delete the user id by receiving Exist form from HR.

- **Responsible and Lawful Conduct**
  - You agree to use the systems and network in a way, which supports and promotes the Bahrain Polytechnic's business objectives. By using the Bahrain Polytechnic's ICTS resources, you agree that information you post on or distribute through the systems or network contains:
    - No obscene or indecent material
    - No advertising material or promotional material
    - No material which constitutes libel, slander, or invasion of privacy or publicity rights
    - No violation of copyrights or trademarks
    - No incitement to riot or violence
    - No violation of national or local law

- **Wireless Networks**
  - Access to wireless networks is provided by Bahrain Polytechnic to facilitate users to access the network services. Wireless access will be restricted to users based on the wireless authentication mechanisms instituted at Bahrain Polytechnic.
  - Users will contact the ICT help desk to receive and modify wireless access credentials.

Refer to Desktop Security Guideline

- **Responsible use of Bandwidth**

  - Bahrain Polytechnic is committed to providing adequate network capacity for the business computing needs of the Users. Due to the large volume of information being transmitted through the Bahrain Polytechnic's network, excessive use of the network by a single User or a group can interfere with the requirements of the other Users.
  - Effecting security breaches or disruptions to network communication are prohibited. Security breaches include unauthorized access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
  - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet is prohibited.

- **Internet**

  - The use of Internet services will be limited to Bahrain Polytechnic-related activities only.
    - Usage of instant messengers, chat software, and peer-to-peer/personal file-sharing network utilities are prohibited and subjected to disciplinary action for non-compliance.
    - Users are not allowed to download software from the Internet unless approved by the Director.
    - The downloaded software must be scanned for viruses and executing or installing the software is not allowed unless it is approved by the Director.
    - Connecting to the Internet by using modems on PCs and laptops, and dial-up connections while connected to the entity's network is prohibited. If there is any business need to use the modem, prior permission is required from the Director.
  - Bahrain Polytechnic ICTS Users using the organization's facilities will not indicate their affiliation with the organization in any bulletin board discussions, chat sessions, and other offerings on the Internet.
  - Internet usage should never cause disruption, corruption, degradation, or security breaches over the Bahrain Polytechnic's information system
  - For business reasons, the usage of remote management of machines software (such as WebEx) can be permitted with appropriate approvals.

- Bahrain Polytechnic's computer systems should not be used to install personal web pages or web servers.
- It is relatively easy to spoof the identity of another User on public networks such as the Internet. Before Users release any internal Bahrain Polytechnic information, enter any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed via digital signatures, but in cases where these are not yet available, other means such as letters of credit, third-party references, and telephone conversations may be used.
- Users are reminded that Web browsers leave "footprints" (or cookies) providing a trail of all sites visited by the Users.
- Bahrain Polytechnic reserves the right to block access to any Internet sites that are deemed inappropriate. The ability to connect to a specific web site does not imply that Users are permitted to visit that site.

➢ **Email**

- Personal or non-business use of the Systems is not permitted.
- E-mail content will be subject to the following restrictions:
    - Sending or forwarding statements containing material that is offensive, defamatory, or threatening to others is strictly prohibited
    - Communication of statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything construed as harassing, offensive, or insulting to others based on race, religion, national origin, color, marital status, citizenship status, age, disability, or physical appearance is strictly prohibited
    - Any statements or comments made via e-mail construed as an action of Bahrain Polytechnic will bear a disclaimer
    - E-mail systems will not be used to produce or distribute unsolicited e-mails, spam mails, or make solicitations for personal gain, political or religious causes
- Users of the e-mail system are prohibited to the following:
    - Providing or sharing e-mail ID and password to unauthorized individuals
    - Forging of header information in e-mail (including source address, destination address, and timestamps)
    - Publishing or distributing internal mailing lists to non-staff members

- sending sensitive information through e-mail without adequate measures to protect the attached information from unauthorized access
- Posting of Network or server configuration information about Bahrain Polytechnic ICTS infrastructure to public news organization or mailing lists is strictly prohibited
- Executing any programs (upgrades or patches) received via e-mail from unknown sources
- Registering the entity e-mail address in any public forums or mail lists for personal use
- Forwarding their e-mails without restriction to their private e-mail account since these accounts are less secure
- Sending, forwarding, or receiving confidential or sensitive Organization information through non-Bahrain Polytechnic email accounts. Examples of non-Bahrain Polytechnic e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and emails provided by other Internet Service Providers (ISP)
- Opening e-mails with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, that she/he thinks may contain a virus, instead, the User should call the ICT Helpdesk and inform the incident.
- Sending, forwarding, receiving, or storing confidential or sensitive Organization information utilizing non-Bahrain Polytechnic accredited mobile devices. Examples of mobile devices include, but are not limited to, personal data assistants and mobile telephones
- Using an electronic mail account assigned to another individual to either send or receive messages. If there is a need to read another's mail (while they are away on vacation for instance), message forwarding, and other facilities must instead be used

- It is the responsibility of a User to communicate with third parties within his/her given authority.
- Fax messages sent via e-mail should be considered e-mail messages.
- The e-mail service is to be used for business purposes as a productivity enhancement tool.
- Electronic mail systems and all messages, including backup copies, are property of Bahrain Polytechnic.

- Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for the archival storage of important information. Stored electronic mail messages may be periodically expunged by systems administrators, mistakenly erased by Users, and otherwise lost when system problems occur.
- All incoming/outgoing electronic mail will be screened for viruses.

➢ **BYOD guideline**

This is refer to the BYOD guideline

➢ **Use of Hardware**

- Users of PCs must not themselves:
  - Disconnect or connect any equipment in general and from/to the Bahrain Polytechnic network in particular
  - Remove the outer case of equipment
  - Move PCs or associated furniture in any way which might compromise the ergonomics of the installation or disturb cabling

Refer to Desktop Security Guideline

➢ **Use of Software**

- All software installed on the PC must be owned by Bahrain Polytechnic and installations should be carried by ICT Help Desk only.
- No software may be copied, or made available over a network, for use on second or subsequent PCs, except when explicitly agreed.
- License or registration cards supplied with software must not be signed and must be returned to the ICT Help Desk.
- Breach of copyright of a software package may render the User liable to prosecution and/or subject to internal disciplinary procedures.

➢ **Security**

- Safeguard all diskettes, tapes, portable equipment and other computer readable media to prevent loss, misuse or corruption of business data.
- Ensure that if the PC is left unattended it is either switched off or locked with a password by the installed standard screen saver.

- All running applications should be logged off or locked at the end of the working day. If all the applications are logged off it is recommended to switch off the equipment.
- Never reveal your password or leave the system unattended while a third party company personal is working on your computer system.
- At login time, if available on the system, every User will be given information reflecting the last login's time and date. This will allow unauthorized system usage to be easily detected.
- Ensure that the passwords of PCs, LAN and applications are kept confidential and changed regularly, in line with the Password standard.
- A computer virus is an unauthorized program, which replicates itself and spreads onto various data storage media (e.g. floppy disks, magnetic tapes) and/or across a network. The symptoms of virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system. Because viruses have become very complex, Users must not attempt to eradicate them without expert assistance. If Users suspect infection by a virus, they must immediately stop using the involved computer and call the ICT Help Desk. Users are prohibited from attempting to eradicate a computer virus from their system unless they do so while in communication with a systems administrator or ICT Help Desk personal.
- It is the responsibility of all Users to take the following actions to prevent infection by and spread of computer viruses:
    - All virus incidents and cases or suspects of virus detection, must be reported to the ICT Help Desk immediately
    - Diskettes sent, and files (attachments) transferred electronically, from Bahrain Polytechnic offices must be virus checked before dispatch
    - Virus checking must be carried out using the virus scanning software installed on each PC

➢ **Cyber Security Staff Training**

- It is critical that staff understand the common forms of cyberattacks and receive training on how to deal with such attacks. Staff should be educated on the applicable cybersecurity awareness.
- Staff training cover the following:
    - Security Awareness Email every month or when it is necessary
    - Cybersecurity workshop

- **Password**

  Refer to Password Security Guideline

- **Audit Trail and Logging**

  - All transactions are auditable or traceable to their origin or source. Audit trails are maintained to provide accountability for all access to secret and confidential information and software and for all changes to automated security or access rules. A sufficiently complete history of transactions is maintained for each session involving access to confidential or sensitive information to permit an audit of the system by tracing the activities of individuals through the system.
  - All computer systems running Bahrain Polytechnic production application systems include logs that record, at a minimum the following data:
    - User session activity including User-IDs, log-in date/time, log-out date/time, and applications invoked
    - Changes to critical application system files
    - Additions and changes to the privileges of Users
    - System start-ups and shut-downs
    - Sensitive transactions
    - List all successful and unsuccessful login attempts
    - ICTS Governance performs a review of the security violations on a frequent basis and requests through the ICT Helpdesk system

- **Physical Security**

  - Physical access controls Bahrain Polytechnic buildings are intended to restrict the entry of unauthorized persons. Users must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances.
  - Visitors to Bahrain Polytechnic areas must be escorted at all times by an authorized employee, consultant, or contractor. This means that an escort is required as soon as a visitor enters a controlled area, and until this same visitor goes outside the controlled area.
  - Users in possession of laptop, portable computer, personal digital assistant, or mobile computer devices for business purposes will safeguard the equipment in his/her

possession, and will not leave the equipment unattended without ensuring prudent security measures.

- **Reporting of Incidents and Problems**
  - All Users will contact the ICT Help Desk for reporting, follow-up and resolution of Information System related incidents and problems. Any information system events or any observed or suspected security weaknesses in information systems or services must be reported to the ICT Help Desk as quickly as possible.
  - Any Users who discover that they have connected to a web site that contains explicit, racist, violent, or other potentially offensive material should immediately disconnect from that site. The Users must report this incident to the ICT Help Desk.
  - All employees must promptly report to ICT Helpdesk any loss of or severe damage to their hardware or software. For example, if a portable computer is stolen, this must be reported.
    This is in line with Incident Management Procedure

- **USB and External Storage and Port Management**
  - Antivirus & Auto-Scanning
    - All Bahrain Polytechnic systems must have real-time antivirus/malware protection enabled.
    - External storage devices are automatically scanned upon connection.
  - User Responsibility Declaration
    - Bahrain Polytechnic users are responsible for ensuring devices used do not contain malicious or unauthorized content.
    - When using USB devices, Bahrain Polytechnic users must use official devices and allow antivirus scans to complete before opening any files.
    - Desktop Security guideline includes sections regarding responsible use of external media.
  - Security Awareness & Training
    - Risks of infected USBs
    - Safe practices for data transfer
    - Handling of sensitive data on removable media
  - No Permanent Storage Use
    - USBs should be treated as temporary transfer tools and not for long term storage or backup of work-related data.
  - Report threats Immediately
    - Any suspicion of malware from USB use must be reported immediately to the ICT Helpdesk team.

Guidelines: Automate Definition

Policy Reference: Information and Communication Technology Services C/IT/007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

The purpose of this guideline is to define 'automate' as below:

Fully automated: a fully automatic process or mechanism enables it to process a task without the need to be constantly operated by a person.

Partially automated: partially automated is a term for process or technology applications where human input is minimized or reduced for day-to-day operations.

Online services: An online service is an entity that provides access to various types of data for different uses via the Internet.

Scope

Based on the above definition for automation, this guideline applies to Bahrain Polytechnic's different processes/mechanisms/technology.

Guideline Statement

- **General Information**
  - **Fully automated:** This level represents a system that has turned to full autonomy, in which human input is optional. We refer to this as a fully automated system. Some characteristics of Fully automated are:
    - The system has sufficient insight into organizational requirements that no longer require human input.
    - Organizational requirements are automatically met without exception.
    - Human involvement is never required.

  - **Partially automated:** Partial automation represents a system in which infrastructure concepts such as code are used, including the principle of using a common approach; this type of automation is called partially automated. Some characteristics of partially automated are:
    - Enhances responsibility in the environment as these changes can be easily tracked.
    - Organizational flexibility improves because the human intelligence required to perform deployments and configurations is captured in machine-readable form.
    - Reduces human interactivity requirements for day-to-day operation.

  - **Online services:** For Online Service provides tools that permit its users to communicate with each other and access sites and information related to their business.
    Examples of online services include online payment, education, online registration, computer help sites, social media networks, and e-mail.

- **Bahrain Polytechnic services**

Below are examples of 'automate' services within Bahrain Polytechnic.

Services	Fully automate	Partially automate	Online services
Learn portal	No	Yes	Yes
Interactive report for Banner document generation usage	Yes	NA	NA
Web-based Strategic Report	No	No	Yes

Guidelines: Periodic Access Review

Policy Reference: Information and Communication Technology Services C/IT/007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

A user or account access review is part of the user or account management, which requires a periodic review of access rights for all employees and vendors. A user access review usually includes a re-evaluation of, User roles, access rights and privileges, and credentials provided to users to perform activities.

Reviewing user access mitigates a wide range of cybersecurity issues as but not limited to:

- Excessive access privileges (privilege creep)
- Mistakes with user role and account configuration
- Access abuse and misuse

The ultimate goal of the periodic access review is to reduce the risk of a security breach by limiting access to critical data and resources without impacting on daily business activities.

Scope

This guideline applies to all Bahrain Polytechnic Managers/Directors who use Bahrain Polytechnic resources (services/software/system).

Guideline Statement

- **General Information**
  - This report is periodically conducted at the beginning of every year.
  - The information or report should contain the user name, role (access to which class or group,..), and the user privilege (read, write, Modify).

- **Access Review Process**
  - At the beginning of the year send information emails through ICT Helpdesk about the report to Managers/Directors of every Department/Directorate.
  - The ICT Quality team has raised a Service Request from ICT Helpdesk to all Managers/Directors with the related report to every Department/Directorate.
  - ICT Quality team calls for a meeting with each Manager/Director if required.
  - ICT Quality team will receive email notifications through ICT Helpdesk while Managers/Directors review the report and send their feedback.
  - Based on the feedback received, the ICT Quality team will act such as but not limited to:
    - If the report is reviewed completely (confirm/delete/add/update) then the ICT Quality team will forward the report for action to a different section within ICT.
    - If the received report is not complete and Managers/Directors ask for more information to be added by ICT, then ICT quality team will update the report and then send it to them through ICT Helpdesk Service Request.
  - Finally, after taking action the report with related Service Request number will archive as evidence for further review.

Guidelines: Incident Management

Policy Reference: Information and Communication Technology Services C/IT/007
Version: 4
Person Responsible: Information and Communication Technology Services Director

Purpose

This guideline aims to ensure the consistent and professional management of information technologies/security incidents to mitigate or minimize any harm to users, information systems and its related devices at Bahrain Polytechnic (BP).

Scope

The guideline applies to all incidents that occur within the organization, including but not limited to cybersecurity incidents, service disruptions, data breaches, and physical security breaches.

Guideline Statement

- **Incident Response**
  - All BP users are responsible for reporting actual, suspected, threatened and/or potential information security incidents to ICT Helpdesk through a call (Phone: 179817111, Ext: 7111) or by using ICT Helpdesk portal.
  - BP user's management is responsible for ensuring that staff in their area act in compliance with all information security requirements and following the procedures of reporting information security incidents.
  - Service Level Agreement_Incidents_v4 clarify incident response for different types of incidents.
  - Where applicable, in the event of critical incidents, infected information systems shall be disconnected from the BP's network until the incident has been resolved and risks sufficiently mitigated.
- **Incident Reporting and Communication**
  - ICT Helpdesk channels for reporting incidents, both internally and externally through below channels:

a. ICT Helpdesk phone: **1789 7111** if you call from mobile or **ext. 7111.**

b. Helpdesk portal: portal/ to raise incidents or requests

- ICT Helpdesk portal/system to track and document incident details, response actions, and outcomes.
- ICT Helpdesk SLA (Service Level Agreement_Incidents_v4) and workflow to ensure timely and accurate updates are provided to stakeholders, including employees, customers, partners, and regulatory authorities.

- **Incident Identification and Classification**
  - Classify incidents based on severity and impact to prioritize response efforts. Based on Service Level Agreement_Incidents_v4.
  - Develop an incident classification matrix that defines incident categories and associated response actions, based on Service Level Agreement_Incidents_v4.
- **Incident Triage and Investigation**
  - ICT email announcement about the incident interruption when applicable.
  - ICT Quality team need to raise a Post Incident Report for all planned/unplanned incident and do investigation to determine the root cause and extent of the incident.
- **Incident Mitigation and Recovery**
  - Risk Management Work Instruction, implement measures to mitigate the impact of the incident.
  - Follow backup guideline and restoration matrix if required system restoration and date recovery.
- **Lessons Learned and Continuous Improvement**
  - ICT Quality team/ICT Responsible team need to raise a Post Incident Report for all planned/unplanned incident, identify areas for improvement, and capture lessons learned.
  - Document recommendations (remediation steps) and update the incident report accordingly.
  - Provide awareness to staff about incident management best practices and their role in incident response.

Guideline: Information Access Restrictions Guideline

Version: 1
Person Responsible: Information and Communication Technology Services Director

Purpose

To ensure access to Bahrain Polytechnic's information systems is restricted based on business requirements, role responsibilities, and authorization, thereby minimizing the risk of unauthorized access.

Scope

This guideline applies to all users, including employees, contractors, consultants, and third parties who require access to Bahrain Polytechnic's ICT resources.

General Information

- All user access to Bahrain Polytechnic's ICT systems must be based on business role, need-to-know, and least privilege principles.
- User account creation, modification, and deactivation is processed through the ICT Helpdesk system under the 'Staff Account Management' service in the Service Catalog.
- Access requests must be approved by HR Directorate and request by the HR Recruitment Team before provisioning for any new staff.
- Access requests must be approved by Department Directorate/Manager and for any Consultant, Contractor or Third Party.
- Privileged or administrative access is subject to separate risk review and requires dual approval.
- User accounts must be linked to individual identities—shared or generic accounts are prohibited unless explicitly authorized and monitored.
- Bahrain Polytechnic's Staff access rights must be reviewed periodically by ICT Governance and updated in case of role change or transfer (link to Periodic Access Review Procedure).
- All access records, request history, and approval workflow are logged and stored in the ICT Helpdesk system.
- Upon user exit or role termination, accounts must be disabled within 24 hours and removed from all group memberships.

Role and Responsibility

Role	Responsibility	Supporting Records
ICT Infrastructure	Provision and disable user access as per Helpdesk workflow.	ICT Helpdesk Tickets, Audit Logs
ICT Governance	Bahrain Polytechnic's Staff Access Review	Elimity and ICT Helpdesk
Department Director/Manager	Approve access requests for users (Contractor, Consultant, Third Party) under their supervision.	ICT Helpdesk Request Approvals
HR Director/HR Recruitment	Inform ICT of new employee exits or role changes.	ICT Helpdesk Request
All Users	Use only assigned accounts and report any unauthorized access.	User Acknowledgments

Guideline: Information Classification and Labelling Guideline

Version: 1
Person Responsible: Information and Communication Technology Services Director

Purpose

To define the process for classifying and labelling information at Bahrain Polytechnic to ensure proper handling, protection, and dissemination of institutional data in accordance with its confidentiality, legal, and business value.

Scope

This guideline is related to ICT and applies to all staff, contractors, and third parties involved in creating, handling, storing, or transmitting ICT information under the ISMS scope.

General Statement

Classification Level	Definition / Criteria	Examples and Labelling
Public	Information approved for public dissemination. No adverse impact if disclosed.	Marketing brochures, website content. Label: 'Public' (optional)
Internal	Operational information intended for internal use. Unauthorized disclosure could cause minor disruption.	Internal memos, training guides. Label: 'Internal Use Only'
Confidential	Sensitive information where unauthorized disclosure may cause legal or reputational harm.	Student records, financial data, HR files. Label: 'Confidential'
Restricted	Highly sensitive institutional or regulated data. Unauthorized disclosure may result in significant legal and operational risk.	Audit reports, system credentials, security plans. Label: 'Restricted'

Role and Responsibilities

Role	Responsibility	Record
Information Owner	Classifies data based on sensitivity and impact	Data Classification Sheet
Information Security Specialist	Guides labelling methods and ensures classification scheme is enforced	Compliance Checklist
End User	Handles and labels documents as per classification	Email/document headers
ICT Governance Team	Monitors implementation of classification and labelling standards	Audit Log, Awareness Records

Procedure: Remote Working Procedure

Version: 1
Person Responsible: Information and Communication Technology Services Director

Purpose

To define the requirements and responsibilities for securely accessing, processing, and managing Bahrain Polytechnic information assets while working remotely, ensuring that information security risks are effectively managed.

Scope

This procedure supports compliance with ISO/IEC 27001:2022 Control A.6.7 for protecting information processed outside the Bahrain Polytechnic's premises and refers to the BYOD Guideline for management of personally owned devices.

Procedure

General Statement

- Personal devices (BYOD) may only be used in compliance with BYOD Guideline.
- Monitor remote access activities for suspicious behavior.
- The Requester (Staff) need to report any remote working related incidents immediately to ICT Helpdesk.
- The Requester must follow Cybersecurity Guideline to ensure safe practices such as locked screens, updated antivirus, and secure Wi-Fi networks.
- Remote access is available to all full time staff whose job functions require access to systems/services outside the office and this is in subjected to approval by the HR department/staff's direct manager.
- Remote access will be automatically revoked after the approved duration unless revalidated by the line manager / the HR.

Activity	Responsibility	Record
Requester must raise a service request via the **Motadata ICT Helpdesk** system.	The Requester	ICT Helpdesk

The request must include a **clear and reasonable justification** for remote access, specifying: • The nature of work • Access duration • System/service/data that need to be accessed remotely.		
Review and approve/reject the request based on necessity, role, and associated risk	The Requester's Director/Manager	ICT Helpdesk
Receive Notification email with either Approval/Reject	The Requester	ICT Helpdesk
Mandate RDS use for all remote access to Bahrain Polytechnic resources.	ICT Infrastructure Team	RDS Usage Logs
Enforce multi-factor authentication (MFA) for all remote logins.	ICT Infrastructure Team	Authentication Compliance Records
Reply the request after the remote working access permitted	ICT Infrastructure Team	ICT Helpdesk
Notification email to the Requester	The Requester	ICT Helpdesk
Close the request with a proper command	ICT Infrastructure Team	ICT Helpdesk

Version Control

Version	Date	Description of Changes	Approved By
5	24 Sep 2025	**Update:** Procedure: Managing ICT Incidents P-C-IT-007.001 based on NAO request Guideline: Bring Your Own Device (BYOD) Guideline: Desktop Security Guideline: Cyber Security **Add New:** Guideline: Information Access Restrictions Guideline: Information Classification & Labeling Procedure: Remote Working	

Appendix

- Risk Management Work Instruction

Risk Managment Work Instruction v0.

- New academic year Computer Labs preparation v1.0 – Flow Chart

Labs and computers readines

- Post Incident Report Template

Post Incident Report Template v0.

- Incident SLA

Incident SLA in Motadata.docx

Confidentiality Agreement (User Acceptance) Form

User Acceptance

All employees who have access to the Bahrain Polytechnic information or information processing resources should indicate their acceptance of Bahrain Polytechnic's 'Cyber Security Guideline' associated with this access. This indication is evidenced by signing this acknowledgement slip.

By signing, the User states that, he/she has understood and agrees to abide by Bahrain Polytechnic's End User Information Security Standards and that the User understands and accepts his/her responsibilities when accessing Bahrain Polytechnic's information and/or information processing systems.

User Acknowledgement:

I, _____ _____, hereby confirm that I have read, understand and accept my information security responsibilities. I also agree to abide by the Bahrain Polytechnic's 'End User Policies'.

Staff ID: _____

Signature: _____

Date: _____