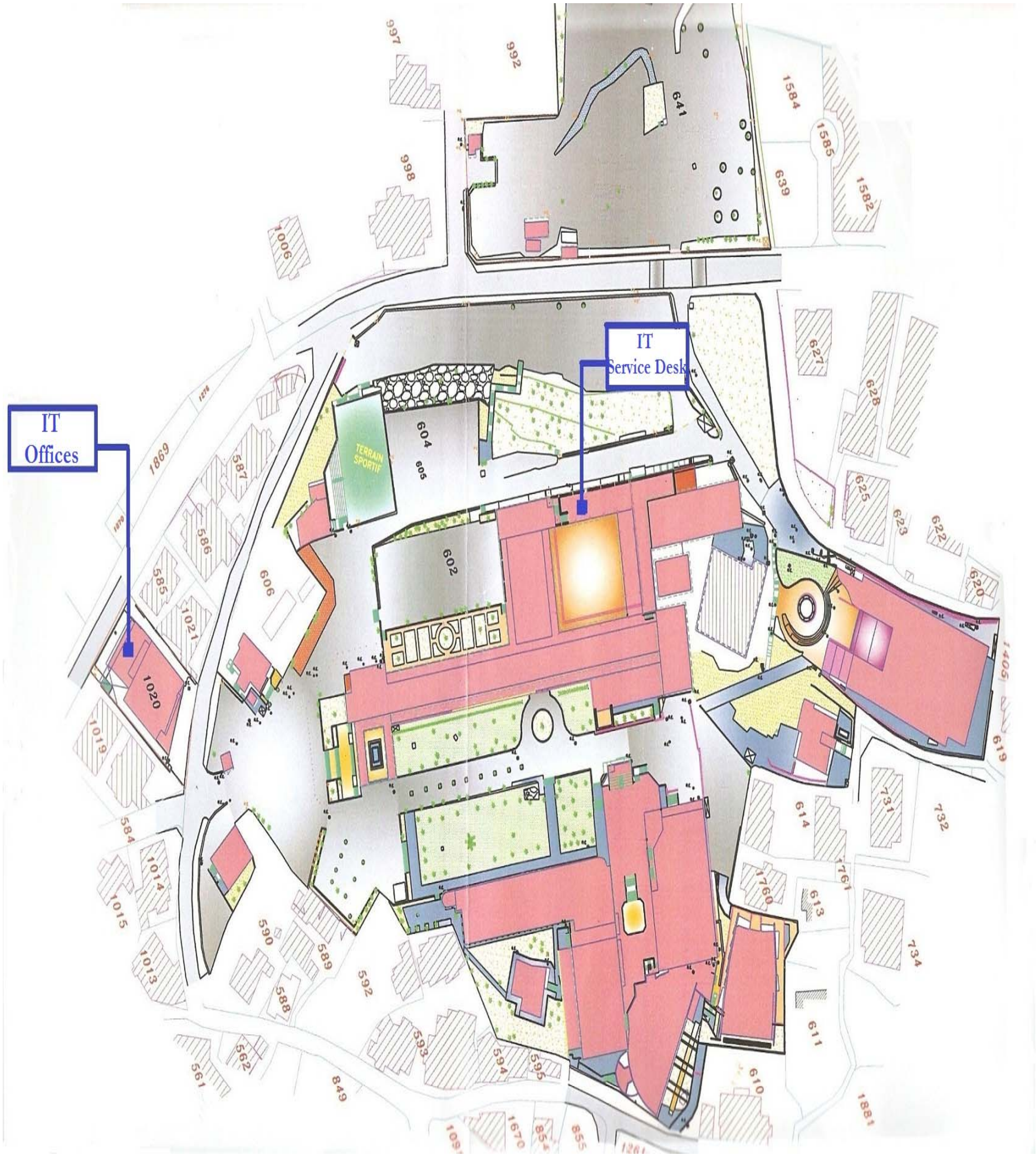
USEK

HOLY SPIRIT UNIVERSITY OF KASLIK

ICT Service Catalogue

Reference Guide

The Staff guide to IT Services


IT
Offices
IT
Service Desk
TERRAIN
SPORTIF
997
992
641
1584
1585
1582
639
998
1006
627
628
625
623
622
620
1406
619
604
605
602
606
1869
587
586
585
1021
1020
1019
584
1014
1015
1013
590
589
588
592
593
594
595
562
561
849
614
731
732
1761
1760
613
734
611
610
1881
1670
854
855

Introduction:

Welcome to the staff guide of ICT services in the Holy Spirit University of Kaslik. The following guide will give you an introduction to the IT facilities available, the information you need and places to get further help. In addition, your obligations as a user are listed.

1.1 USEK encourages the use of electronic communications to share information and knowledge in support of the University's mission and to conduct the University's business. To this end, the University supports and provides interactive electronic communications services and facilities, such as telephones, electronic mail, Lync, video conference, and electronic publishing services such as the internet.

1.2 These communications services rely on underlying voice and data networks delivered over both physical and wireless infrastructures.

Policy Statement:

Information and communication technology (ICT) is provided to support the teaching, learning, research and administrative activities of the University. The data held on the network forms part of its critical assets and is subject to security breaches that may compromise confidential information and expose the University to losses and other legal risks.

Users are encouraged to refer to the online university policies on MyUsek (Mypage).

These regulations are reviewed and approved by the information technology committee.

Purpose:

The ICT guide has been established to:

1. Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources, provided for use by academic, professional and staff, in support of the mission of the University.
2. Protect the privacy and integrity of data stored on the University network.
3. Mitigate the risks and losses from security threats to computer and network resources, such as virus attacks and compromises of network systems.
4. Reduce interruptions and ensure a high availability of an efficient network, essential for sustaining the business of the University.
5. Encourage users to understand their own responsibility for protecting the University network.

Audience:

These regulations apply to:

1. Users (academic, staff, students and others with extended access privileges) working on either personal or University - provided equipment, connected locally or remotely to the network of the University.
2. All devices connected to the University network, irrespective of ownership.
3. All external entities that have an executed contractual agreement with the University.

Acceptable Use:

1. The University provides electronic communication systems and services to all staff, in support of its professional mission. The use of these facilities is subject to limitations necessary for the reliable operation of the electronic communication systems and services.
2. The electronic resources should be used for the purpose for which they are intended.
3. Users must respect the rights, privacy and property of others.
4. Users must adhere to the confidentiality rules governing the use of passwords and accounts, details of which must not be shared.
5. Temporary passwords provided by the IT to users must be changed immediately, following a successful login.
6. Personal use:

   6.1 The university network and computing resources may be used for incidental personal purposes provided that:

   6.1.1 The purposes are of a private nature, not for financial gain and do not break any other policies.

   6.1.2 Such use does cause noticeable cost to the University.

   6.1.3 Such use does not inappropriately interfere with the official business of the University.
7. Users must comply with all applicable laws.

Unacceptable Use:

1. The university ICT facilities must not be provided to individual consumers or organizations outside the University.
2. Use of a username and password belonging to another user is unacceptable.
3. There must be no attempts to crack passwords.
4. Intentional creation, execution, forwarding or introduction of any viruses, worms, Trojans or software designed to damage the performance of the University network is forbidden.
5. It is unacceptable to connect any computer device to the University network, unless it meets the security standards established by the IT department.
6. Interference with or gaining illegal access to user accounts and data, including viewing, modifying, destroying or corrupting the data belonging to other users is unacceptable.

7. It is forbidden to download, store and disseminate copyrighted materials, including software and all forms of electronic data without the permission of the holder of the copyright or under the terms of the licenses held by the University.

Staff Services:

ICT services aim to provide the highest standards of IT services across all the University's campuses, through effective management, development and support.

As mentioned, USEK seeks to provide staff with reliable and secure access to the USEK local network, Internet and to an electronic messaging system via a network of personal computers to facilitate reliable communications and to provide direct access to readily available sources of information for business needs.

What IT services can I expect?

These are the services and facilities you will probably be using at USEK:

- Access to your PC.
- IT Service Desk.
- Your personal email account.
- VDI (Virtual Desktop Interface).
- Application services.
- Access to the internet.
- Intranet.

A. Computer Support

The primary role of the IT Service Desk is to support end users in completing business tasks in a timely and high quality manner. IT Service Desk resolves issues, including hardware, software, PC support, wireless and networking.

To report a problem, you are kindly requested to use one of the methods listed below:

- Send an email to servicedesk@usek.edu.lb.
- Call 1414.

On occasion, it's necessary for desktop computing equipment and user account information to be moved, added, or changed in some way. All these requests must be approved by a designated supervisor, by submitting a request form to the IT Service Desk and must be received a minimum of three business days in advance of the requested action date.

B. Username and Password

Each staff member is given a unique username and password to be used on any system that resides at any USEK facility, in order to have access to the USEK network or any form of access that supports or requires a password.
Passwords are a critical part of information and network security.
Strong passwords promote a secure computing environment; badly chosen passwords endanger the information that they are supposed to protect.

Choosing a password:

- Passwords should contain a mixture of lower and upper case letters, numbers and other characters such as punctuation marks and symbols.
- It must include at least one numerical character.
- A new one must contain, at most three characters from those found in the old password which is being replaced.
- Old passwords cannot be re-used until the user has changed his/her password three times.

Password should not:

- Contain names, words that can be found in dictionaries, words in reverse order, abbreviations, acronyms, or dates of birth.

- Must NEVER be disclosed to others, not even IT staff. Do not allow other people to use your access unsupervised as you will be held responsible for their actions.

- Users must guard against responding to emails asking them to provide their username and passwords for system maintenance. These emails are fake and a clear attempt to steal a user's identity for disreputable purposes.

Changing your password:

You can change your password at any time by pressing ***CTRL+ALT+DEL*** simultaneously. It will lead you to the Windows security popup pane. Select ***change password.***

Before doing it, we strongly recommend that you read the previous section, which describes how to choose a password, since it will help you to create a secure one.

Recovering your account and password details:

Anytime you forget your password, contact Miss Christine Moubarak (by calling 1434), in order to reset it.

C. Email:

Use of email by employees of USEK is permitted and encouraged where such use supports the goals and objectives of business.
Each staff and Faculty member with an email account will be assigned a mailbox on USEK's mail server.

Staff and Faculty members' account names will be FnameLname@usek.edu.lb.

Using email safely:

Whenever you send or receive communications on the internet, there are opportunities for individuals to intercept them and obtain your email address. IT services is there to ensure the campus' email service is secure. However there are some simple steps you can take to play it safe.

- Never open file attachments in email. Always save and check the file with your virus scanner.
- Never install software you receive via email unless you have checked it for viruses and spyware.

Unacceptable actions:

The following actions by an employee are considered unacceptable:

- Use of company communications tools to set up personal businesses or send chain letters.
- Forwarding of company confidential messages to unauthorized third parties.
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic or illegal.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus or malware into the corporate network.

USEK accepts that the use of email is a valuable business tool. However, keep in mind, that the misuse of this service can have a negative impact upon employee productivity and USEK's image.

Email at home or away:

If you wish to use your email whilst you are off the campus, a web-based service is available from any PC, which is connected to the internet.

Open the internet browser and type the URL http://webmail.usek.edu.lb/exchange in the address box, or open USEK website and click on the USEK Webmail button at the top of the page.
Enter your personal username and password as required in the dialog box (for the username, enter: usek\<FnameLname>).

Email attachments and filling Email:

- Limit sending large files so that the e-mail server system does not risk being impaired.
- Instead of sending a message with an attachment to a large distribution list, place it in a shared area and email people with the filename and its location or place it on the University intranet.
- Cleanup of stored messages is your responsibility. From time to time, you should go through your stored messages, deleting those that are no longer needed.

Calendar Services:

This service provides the ability for staff to manage electronic diaries and schedule resources and assets that are managed within their business areas. Support for this service includes synchronisation with personal devices.

How much email space do I have?

Email storage space for individual members of staff is limited to 1 GB, so regular clean-ups are recommended to avoid running out of space.

D. Computer security and your PC:

Up-to-date anti-virus package installed and windows updates enabled.

PC and data protection:

Users are solely responsible of their computer's account. Do not disclose your password to anyone else or display it anywhere visible.

Virus protection:

A virus is a program written to cause intentional damage to computer systems or networks, generally replicating itself from computer to computer across the network (downloaded from the internet or as an attachment to an email message). Moreover it can be perpetuated by the distribution of an "infected" external media device such as CD, DVD or USB flash memory.

A virus infection can be very costly to USEK in terms of data loss and staff productivity.
USEK provides a computing network that is virus free. Including company owned and personally owned computers attached to the USEK network.

However, all users must follow the necessary steps to protect University systems from viruses, by adhering to this rule:

- Any software programs must not be installed or executed without the prior approval of IT services such as: any programs obtained from the internet or any unauthorized program attached to an email message.

E. Virtual Desktop Interface:

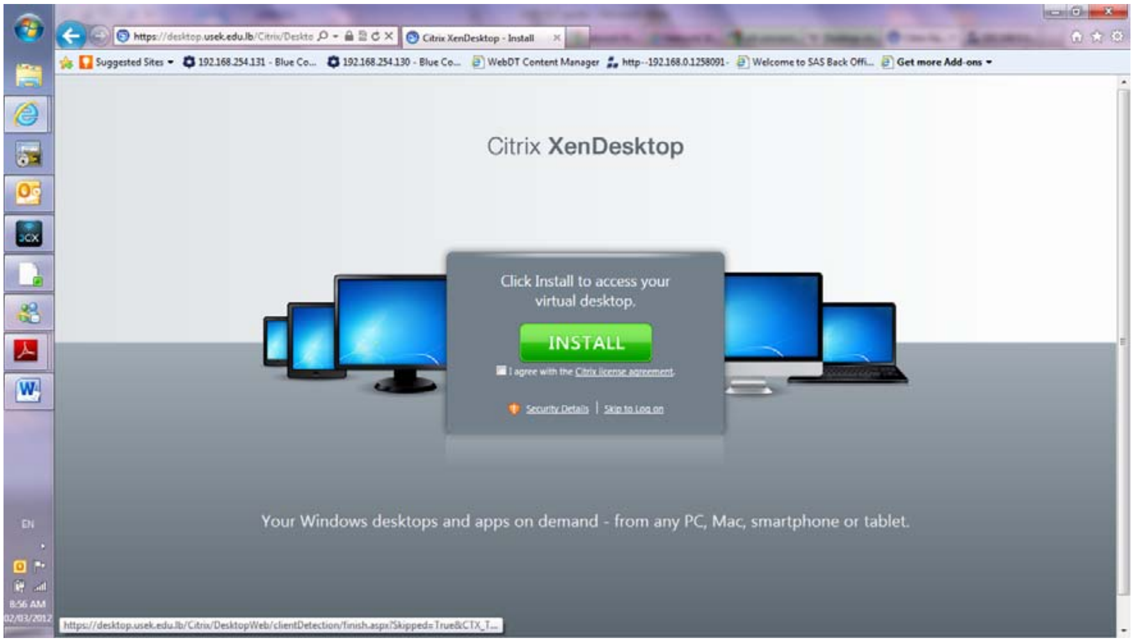
Virtual Desktop Interface is USEK's virtual environment, that can be accessed from anywhere with an internet connection, web browser and windows based computer, thus improving productivity while concurrently tightening data security.

Requesting access:

All USEK staff can have access to VDI, using their standard network account.

To access VDI from campus, please visit https://desktop and follow the prompts.

If you are off campus, type https://desktop.usek.edu.lb



https://desktop.usek.edu.lb/Citrix/Deskto
Citrix XenDesktop - Install
Suggested Sites
192.168.254.131 - Blue Co...
192.168.254.130 - Blue Co...
WebDT Content Manager
http--192.168.0.1258091-
Welcome to SAS Back Offi...
Get more Add-ons
EN
8:56 AM
02/03/2012
https://desktop.usek.edu.lb/Citrix/DesktopWeb/clientDetection/finish.aspx?Skipped=True&CTX_T...

Citrix XenDesktop

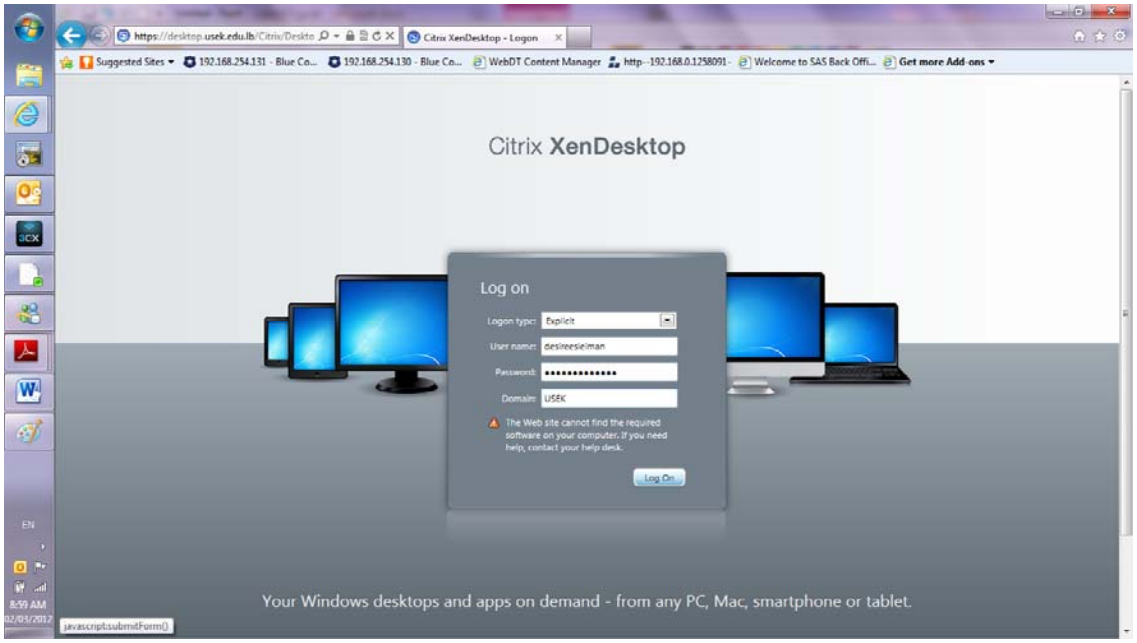
Click Install to access your virtual desktop.

INSTALL

□ I agree with the Citrix license agreement.

Security Details | Skip to Log on

Your Windows desktops and apps on demand - from any PC, Mac, smartphone or tablet.



https://desktop.usek.edu.lb/Citrix/Deskto
Citrix XenDesktop - Logon
Suggested Sites
192.168.254.131 - Blue Co...
192.168.254.130 - Blue Co...
WebDT Content Manager
http--192.168.0.1258091-
Welcome to SAS Back Offi...
Get more Add-ons
EN
8:59 AM
02/03/2012
javascript:submitForm()

Citrix **XenDesktop**

Log on

Logon type: Explicit

User name: desireesleiman

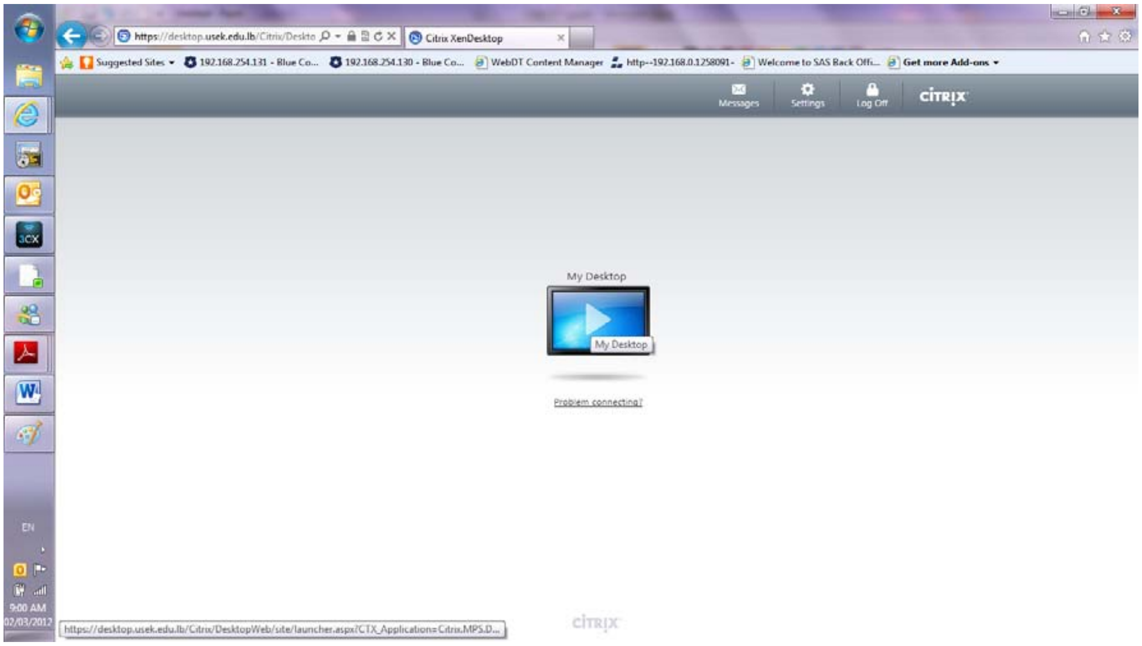
Password: ••••••••••••••

Domain: USEK

⚠ The Web site cannot find the required software on your computer. If you need help, contact your help desk.

Log On

Your Windows desktops and apps on demand - from any PC, Mac, smartphone or tablet.

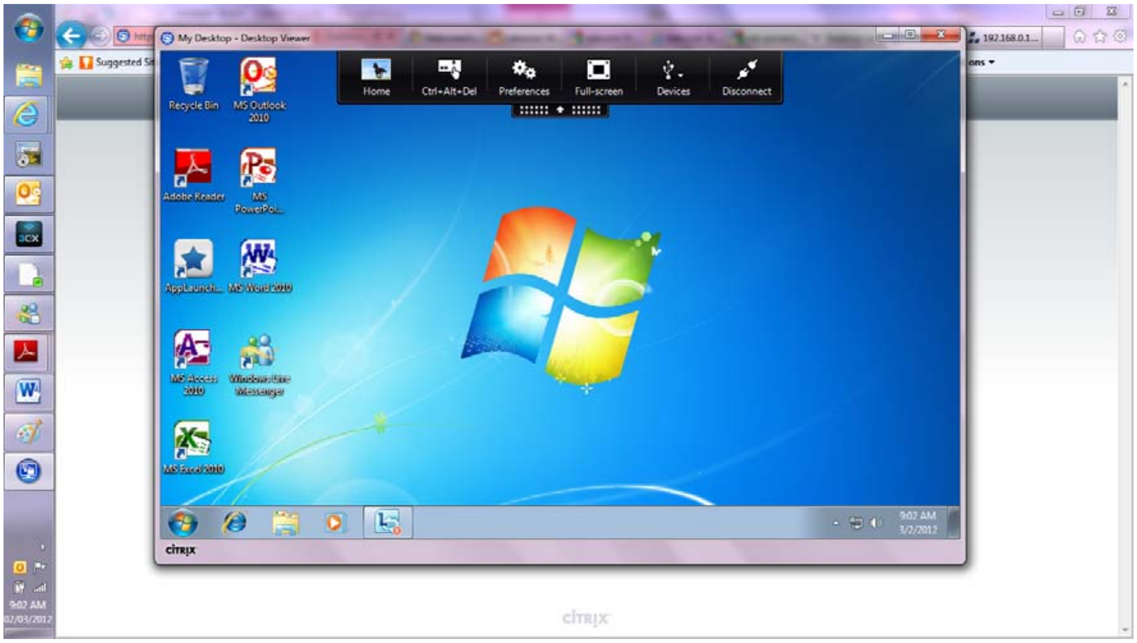


https://desktop.usek.edu.lb/Citrix/Deskto
Citrix XenDesktop
Suggested Sites
192.168.254.131 - Blue Co...
192.168.254.130 - Blue Co...
WebDT Content Manager
http--192.168.0.1258091-
Welcome to SAS Back Offi...
Get more Add-ons
Messages
Settings
Log Off
CITRIX
EN
9:00 AM
02/03/2012
https://desktop.usek.edu.lb/Citrix/DesktopWeb/site/launcher.aspx?CTX_Application=Citrix.MPS.D...
CITRIX

My Desktop

My Desktop

Problem connecting?



<u>**Virtual Desktop interface hosting is more secure:**</u>

IT hosts the desktop on a server where data is kept safe and not on the end-user's machine which can be lost, stolen or corrupted with viruses. VDI lowers the risk inherent in storing data on the user's desktop computer.

VDI improves data integrity of user information because all data can be maintained and backed up in the data centre.

Please contact Mr Elias Abi Jreiche, for assistance regarding VDI.

F. Application services:

Application services include:
1. Application Design and development service
2. Application support
3. Application enhancement

<u>**Application design and development service:**</u>

IT software development and innovation division provides services to design and develop new applications, or significant new functionality for existing applications.

<u>**Application support:**</u>

- Provides delivery and support of business applications used by University staff and students, including resolution of technical issues.

Application enhancement:

- Provides support for various business applications used by the University. It includes upgrades and modifications to supported applications.

Software request:

IT software development and innovation division allows USEK to leverage its computing usage by creating applications specifically customized to its needs and requirements, integrating existing applications and systems, or recommending the purchase of an application, in order to enhance the work and provide a better service to the community; this is through a from request submitted on the intranet portal MY USEK.

G. Access to internet:

The primary purpose of internet availability in USEK is to provide access to information that will enhance and support the educational, instructional and research activities of students, Faculties, and staff.

IT provides the campus community with both wired and wireless access to the University's network as well as to the external internet.

Faculties, staff and visitors can get access by logging in using their USEK username and password.

USEK Users:

USEKwifi will be available at all locations in USEK. Faculties and staff must connect to USEKwifi and then they will be automatically given the appropriate set of permissions, based on the usernames they provide.

USEK Guests:

USEK visitors and guests will be given internet access only through USEKGuest.
USEKGuest is intended solely for internet access.

Features:

- Simple, secure wireless connection.
- Wireless connections available in every building and every office on campus.
- Wired connections available in staff offices, faculties, labs, Central library, etc.
- Access to web sites is monitored and, in some cases, blocked.
- USEK has a quota system that provides staff with an amount of internet usage which is deemed sufficient for their work purposes. As a guide, quota is 75 MB. If this quota is exceeded, your internet access will be slowed.

Mobile devices (including Personal Digital assistant and cellular phones):

Mobile devices can be defined as portable hand held devices that provide computing and information storage/retrieval capabilities for personal or business use.

Developments in technology and the business demands placed on users have led to the introduction of many portable devices to be used to access University resources, such as emails and calendars.

Monitoring:

USEK accepts that the use of the internet is a valuable business tool. However, misuse of this service can have a negative impact on employee productivity and USEK's image.

In addition, USEK's entire internet related resources are provided for business purposes. Therefore, USEK maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

H. Backup retention:

Establishes the structures that exist around data management; backups, retention, destruction and retrieval of data and documents.

Since data is one of USEK's most important assets, it is imperative that it be safely and securely captured, copied and stored.

The backing up of USEK systems, databases and applications is necessary for the total restoration of the system in the event of major failure.

Deletion of data:

Users should be aware that data deleted from local disks by the users, may still be accessible in some cases, via certain system tools.

However, IT does not recover individual deleted emails unless a request is approved by the department Director; IT backs up the email system for the purpose of restoring the service when it suffers a major system failure, and the whole system has to be restored.

I. Infrastructure and enabling services:

Data center management	Management of data center facilities including physical security, power, electricity, air-conditioning, space and redundancy.
Network management	Management of core, edge and backbone network including redundancy provisions.
Information security management	Provision and management of firewalls, intrusion detection and vulnerability management.
IT policy development	Management of key policies governing IT such as the IT acceptable use and security policy.
Incident management	Management of the incident management process.
Business continuity management	Service that ensures that business processes are maintained in the event of a disaster, by contributing to the University business continuity management plan.

J. Access by external entities affiliated to the University:

1. External entities that have an executed contractual agreement with the University may access appropriate resources and must comply with the University guidelines and policies.

2. Any external visitors or conferences that have been authorised to use the University ICT facilities are bound by University guidelines and policies and are liable for the actions of the attendees.

Conclusion:

The IT department has the operational responsibility for the University network and central computing resources, and it has an obligation to protect the confidentiality, integrity and availability of the network by ensuring that the resources are available and accessible.
To meet this obligation, the IT department may monitor and respond to network breaches as they occur.

The University is committed to the provision of efficient and effective administrative support to serve the needs of the whole University. For this particular purpose, detailed documents about University policies are available at MYUSEK and are considered to be a definitive reference source for all staff.

Guidelines and policy references:

a. Antivirus Policy.

b. Application Server Provider.
c. Application Server Provider Standards.
d. Audit Vulnerability Scanning Policy.
e. Data Protection Policy Enduser.
f. Downtime policy.
g. Move/Add/Change Policy.
h. Password Policy.
i. Servicedesk Triage Policy.
j. Software Request Policy.
k. Third-Party Access Policy.

Please note that the IT Department is still developing new policies.