The EdITion 2

Your info guide to ICT Support

www.ufs.ac.za/ict

UFSUV | UFSweb | UFSweb | ufsuv

Inspiring excellence, transforming lives through quality, impact, and care.

UNIVERSITY OF THE FREE STATE
UNIVERSITEIT VAN DIE VRYSTAAT
YUNIVESITHI YA FREISTATA

UFS
INFORMATION AND COMMUNICATION TECHNOLOGY SERVICES (ICT SERVICES)

Content page

Introduction

There is so much Information and Communication Technology (ICT) material available, that you may find yourself going in circles while looking for the answers that you need. Hence, we compiled an easy-to-read e-publication for the University of the Free State (UFS) community with information that you can trust.

Experts from our ICT department contributed insights within their specific knowledge fields that are relevant to you – the user. Since we want you to read and digest the content, we limit the number of articles, and increase the publication frequency.

In this edition we address the hurdles and solutions of remote working, improving research with high-performance computing, and digital security. We also unpack our IT services framework and Information and Communication Technology Services (ICTS) Ops Centre so that you know what happens behind the scenes and how to access support.

We would also like to remind you that ICT Services is committed to providing a conducive digital future in terms of platforms, infrastructures, systems and associated digital services to launch the UFS into the digital future it aspires to.

If you have any additional questions about the content shared in this publication, or find something of interest that you would like to share with the community or us, please do not hesitate to reach out.

ICT Services Framework

An industry prone to teleworking, digitalisation, and an ever-evolving customer base means it is no longer possible to deliver an all-inclusive tool or service immune to digital advancement and change. The opportunities and possibilities posed by the wide range of products and services are just too extensive.

The rapid pace at which these changes are occurring also impacted and somewhat changed the traditional role of IT. The relationship you have with your IT department has shifted from a guy who stops over to sort out your hardware and software problems to becoming a service that is much more personal. IT in this new era has become a partner in enabling you to execute strategy and become more efficient. Without tools that are fit for purpose, it becomes very challenging for individuals and businesses to reach stakeholders that function in a digital world.

ICTS at the UFS supports the notion of integrated thinking and tools that are fit for purpose. Because the world of IT has changed from inside-out thinking to outside-in thinking, ICTS also had to make some adaptations. The following changes have been made to our services framework to support you going forward:

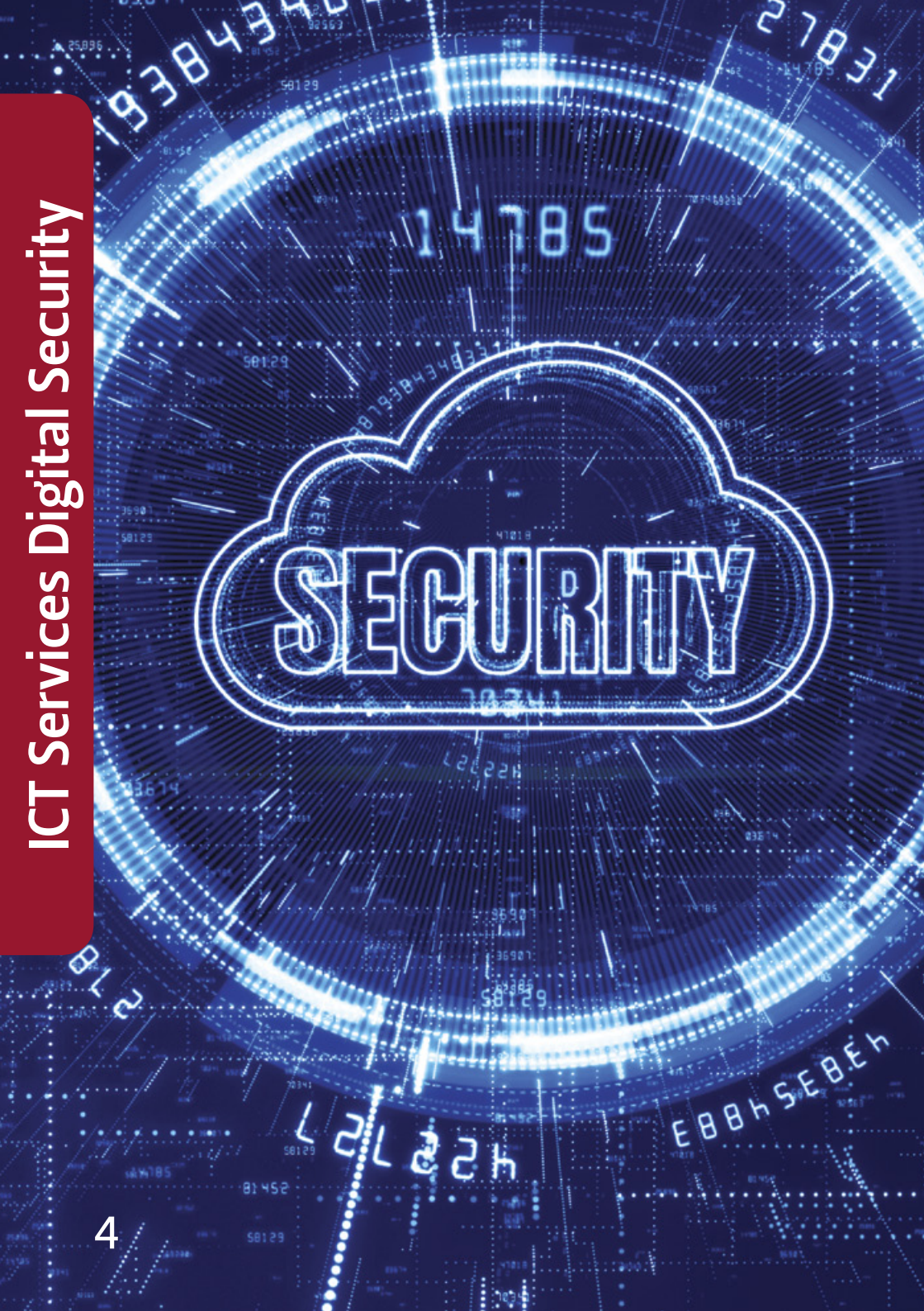
- ICTS is moving from a technology-focused services framework to a service-based framework. These services are structured to invite and support a collaborative approach that informs sustainable outcomes. The changes to the structure have the objective of enabling, supporting and sustaining institutional initiatives optimally.

- The services framework is structured to ensure operational stability and integrity in a changing business paradigm.
- The core of the new services framework prioritises the following objectives:
    - Digital (Information) Security
    - Effective Data Management
    - Risk, Governance and Compliance
    - Business Enablement
    - Operational Integrity

To find out more about each of these services, visit our ICTS website or feel free to send an email to kotzejj@ufs.ac.za.

Also, be on the lookout for the follow-up article that will detail a foolproof step-based approach to support your local IT technician.

The opportunities and possibilities offered are just too broad and appealing to stick with one solution.


SECURITY

UFS ICT Digital Security: What you do online matters

Most people are under the erroneous impression that their online activities are conducted "anonymously". In reality, the opposite is true – everything that you do online has a footprint (often permanent), and every online activity has an effect or a reaction. In order to keep our working environment safe and productive, the University of the Free State (UFS) has several regulations in place for your online activities.

During the past two years, most of our lives have moved online – and we are grateful that teaching, learning and working could continue in this way. However, the lines between professional (work-related) and private (personal) online activities have become blurred. It is important that our staff maintain a regulated online presence, especially when it comes to e-communication and browsing.

Electronic messaging covers email and various forms of instant and store-and-forward messaging such as SMS texts, messaging apps, webchats and messaging facilities on social media platforms. For professional use, and while using UFS devices, you are only permitted to use university-provided electronic messaging facilities. Note that all university messages should be considered official communication from the UFS and treated as such. Do not send messages containing material that is defamatory or obscene, or which a recipient might otherwise reasonably consider inappropriate, including:

- Junk mail
- Copyrighted material
- Possible viruses
- Fraudulent or forged content
- Abusive, discriminating, defamatory, threatening, bullying, offensive, obscene or indecent content
- Content that is anonymous, violates other users' privacy or may cause anxiety


The University of
the Free State has
several regulations
in place for your
online activities.

If you are unsure about a message, check with your line manager before responding or forwarding the content.

Although you are allowed some personal use of the Internet during your own time (such as a lunch break), Internet access on UFS-owned devices is primarily dedicated to work. Work-related activities include accessing UFS systems, research, updating UFS platforms, and other tasks that are part of your role. Although the University has strict security measures in place to protect its online content, inappropriate browsing could result in a breach.

As a UFS employee, you are not allowed to knowingly create, download, upload or display content, or access sites that contain inappropriate material that might be deemed illegal, obscene or offensive. Never download or install software that is not approved by the UFS for use. You may also not run a private business online via UFS devices and platforms.

Digital security is the responsibility of each member entrusted with conducting online activities within the UFS system – one careless act can compromise all. Together, we can keep our data safe.

High-Performance Computing (HPC)

The eResearch and High-Performance Computing (HPC) unit may be able to assist you if you are a researcher experiencing challenges with:

the processing of large data sets, for example next-generation sequencing data;

constant interruptions of computer workflow due to load shedding;

long turnover times for workflows/pipelines that transform data on a repetitive cycle;

machine learning/deep learning or artificial intelligence for research.

The generation of massive amounts of data has become inextricably linked with many modern research techniques in various research areas. However, this also means that the computational resources needed to process, transform and integrate this data into research projects far exceed what desktop computers can offer.

This is where the UFS HPC unit steps in. An HPC system is a collection (cluster) of servers connected to one another. This enables a researcher to use multiple computers simultaneously to accelerate a computational workflow. Whereas a high-performance desktop system can typically provide a CPU with 12–16 cores, 16–32 GB of RAM and approximately 12 TB of storage, on the UFS HPC system, one server (or node) alone provides 64 cores and up to 1024 GB of RAM. Storage is provided via a storage server with 1400 TB of usable storage, which is also fully backed up.

Of course, a researcher may utilise many nodes at once. For example, a researcher accelerated Molecular Dynamics simulations of a nucleosome system that contained about 1 million atoms using 192 cores across six nodes on the UFS HPC system. A simulation that would have taken approximately 17 years on a workstation computer was completed in 3 months. This allowed the researcher to perform eight such simulations throughout their doctoral study.

In another instance, a researcher required well over 512 GB of memory for genome assembly and achieved this using one of the nodes on the UFS HPC system, which provided 1024 GB of RAM.

In recent times, GPUs (Graphical Processing Units) have gained prominence due to their use in artificial intelligence and machine learning. The UFS HPC system also provides nodes with these accelerators. For example, the UFS HPC team have set up AlphaFold, a protein structure prediction tool that utilises machine learning accelerated on GPUs. This tool has revolutionised the protein prediction landscape and recently received widespread acclaim and media coverage. However, even though the software is freely available, it requires about 3 TB of storage for its data sets (a compressed download of about 400 GB) and a GPU to accelerate the prediction calculations. Thus, UFS researchers have access to this cutting-edge tool (which is practically inaccessible to the average researcher) thanks to the UFS HPC unit.

The examples above only scrape the surface of the UFS HPC system's potential to unlock new research avenues in various research areas. While the acceleration potential of each research application depends on the software used to solve a particular computational problem, most research projects that contain a computational element can benefit from the UFS HPC system.

A consultation with the UFS HPC unit to accelerate and unlock your research potential can be requested by sending an email to: **hpc@ufs.ac.za.**

Background

Network Operations refers to the actions conducted by internal networking staff or third parties on which corporations and service providers rely to monitor, manage, and respond to alerts on the availability and performance of their network. Staff that are primarily responsible for network operations are commonly referred to as network operations analysts or network operations engineers.

A Network Operations Centre (NOC) is a centralised place where network operations staff offer 24/7/365 supervision, monitoring and control of the network, servers, databases, firewalls, devices and relevant external services. This infrastructure environment might be on the premises or hosted by a cloud provider.

Network Operations Centre (NOC)

The NOC is the ICT Services unit function that is in charge of ensuring that the University of the Free State (UFS), IT network infrastructure can satisfy the demands of the company. The corporate network is used for specific reasons by each company, and the NOC optimises and troubleshoots the corporate network to ensure that it can satisfy the demands of the business.

Objectives of the NOC

Ensure that the corporate network is able to meet the needs of the business.

Take corrective action to reduce the effect of service outages and system failures.

Recognise the infrastructural components accountable for service delivery.

Provide information on component or service trends that may be utilised to improve UFS ICT Services performance.

Goals of the NOC

The goals of service monitoring and control include the following:

- Observe the system health status of UFS ICT Services.
- Take corrective action to reduce the effect of service outages and system failures.
- Recognise the infrastructural components accountable for service delivery.
- Provide data on components or service trends that may be utilised to improve ICT Services performance.

Working Remotely

At this point, I think everyone is tired of hearing about "the new normal". Over the past two years, all UFS staff and students have been forced to rapidly adopt technologies for remote working. Some have found it easy to adapt to these changes, while others may be experiencing stress. In this article, we will discuss some considerations to assist you in navigating the uncertainty of working remotely, and some pointers that you may not be aware of.

A few things to consider when working remotely to make life easier:

Using a laptop will make it easier for you, since you have all your software and documents on hand and the device has a built-in webcam and microphone. Since a laptop will switch over to battery power when the electricity supply is interrupted (due to load shedding, for instance), it also reduces your risk of losing an important document that you were working on.

You should also make sure that you have a good internet connection in the location where you are working from. Many options are available, such as Fibre to the Home (FTTH) and Fixed Wireless, as well as mobile data connectivity via Vodacom, MTN or CellC. Internet service providers normally indicate their network coverage on a connectivity map, which you can easily find by searching on Google. This will give you an indication of whether your prospective service provider has network coverage in your area. It is also a good idea to speak to your neighbours and ask which service providers they are using, and whether they are experiencing any problems.

In view of the ongoing challenges posed by load shedding, it may also be a good idea to invest in a UPS (Uninterruptible Power Supply). This will greatly assist in ensuring that your Internet connection is stable during load shedding, as you can connect your router and fibre connection equipment to the UPS instead of using Eskom power directly.

The UFS also has the GlobalProtect VPN with reverse billing in place. This was introduced to enable emergency remote learning during the advent of Covid-19, back in April 2020. This mechanism allows you to connect to various resources without incurring costs on your cellular network. To make use of this, you only need to install the GlobalProtect software on the device that you will be using to connect to the Internet (cell phone, tablet or laptop).

Also ensure that you have enrolled for the Duo multi-factor authentication system. Various university systems such as PeopleSoft, Office365, GlobalProtect and RIMS now require you to complete a two-factor authentication process when working remotely. For assistance in this regard, feel free to contact the ICTS Service Desk at x2000.

Various types of disruptions have been experienced at the UFS since 2015, ranging from Fees Must Fall to the Covid-19 pandemic in 2020. UFS departments should plan for future disruptions, and a good strategy may be to equip staff members with laptops as a first option, to enable them to deal with any possible disruptions more easily. Purchasing laptops will be slightly more expensive than a desktop PC solution, but will enable staff to work more efficiently while at home.

Staff members should make sure that they keep their PCs or laptops in a safe place when working remotely to ensure that no sensitive data is lost, and to avoid dealing with any theft or insurance claims.

We wish you good luck with all your remote working endeavours; remember that ICT Services is always there to assist you.

While most UFS staff members have been trained and equipped to work from home or elsewhere, there are still some things you can do to make this experience less stressful.

ICT Services

Log support request by emailing ufs@service-now.com or signing in to SolveIT (http://solveit.ufs.ac.za/) with your campus credentials (username and password)

Service Desk

+27 51 401 2000 | servicedesk@ufs.ac.za

Knowledge Base

It is a repository of best practices and knowledge of services and products offered by ICTS
http://solveit.ufs.ac.za/