CENTRAL
OFFICE OF
INFORMATION
TECHNOLOGY

ITC Updates

April 2024

Campus Phone System

Central updated our phone system in 2016 to Cisco Unified Communications, hosted locally on the campus. The solution has performed well for those 8 years, but as with all technology it's time for a refresh. While the phone devices in our offices are still working well, the backend hardware and gateways are end of life and support. The information technology department has spent the better part of FY24 evaluating our next phone system.

As a result of our current licensing, we evaluated two solutions Microsoft Teams Calling and Cisco Webex Calling. After running pilots of both solutions, in which we accounted for analogy devices (Blue emergency, elevators), 911 services, Call Center services, integration with our Emergency Notification System, softphone vs hard phones, and costs of a fully implemented system, Cisco Webex Calling was the correct decision for Central.

The project to move to the new phone system will begin Spring 2024 and hopeful be completed by early summer. The new phone system will work with our current devices and offer a softphone option. There will be training provided to all staff. The IT team is looking forward to the challenge of a new solution and is eager to service the university community.

New Reporting Tool: Evisions Argos (Replacing Hyperion Workspace)

The Hyperion Reporting system is being retired mid-April. The IT department has moved all the existing Hyperion Workspace reports into our new system, Evisions Argos. Those with access to run Hyperion Workspace reports have been set up in Evisions Argos and may begin using the new system. Details and instructional materials are located here.
You are invited to attend training on how to run your reports in the Evisions Argos Report Viewer. Training is being offered in-person in the TechCentral Classroom, Marcus White Annex Room 102.

Register for Argos Report Viewer Training

Geofencing

The Central IT department is proposing to implement Geofencing to mitigate account compromises by restricting logins to authorized locations worldwide. Given that most of our logins originate from North America, this change must accommodate travel outside of this region. To facilitate this, Central IT will introduce a self-service process allowing staff to opt into international travel (either a form or by logging a support ticket with the Help Desk). Initially, all faculty and staff accounts will default to North America, but individuals may voluntarily enable international access as needed. International access may be maintained indefinitely unless there is a compromise of the account, in which case appropriate measures will be taken. This proposal aims to bolster security while providing flexibility for staff members requiring international access.

If approved by the ITC we will implement in Fall 2024 (October).

Reminder: Never Change your Password Again! New Password Policy Started March 4, 2024

To enhance account security, Central implemented a new password policy that aligns with guidelines set forth by the National Institute of Standards and Technology (NIST). The new policy requires all users to create a passphrase with a minimum of 16 characters. A passphrase is a type of password that is generally longer than a traditional password and can contain spaces in between words such as: "The sky is very blue today". Like a traditional password, a passphrase can also contain numbers and symbols (though not required). By utilizing longer and more complex passphrases, consisting of random words or phrases, password theft becomes more challenging, thus minimizing the risk of your account being compromised. The use of passphrases also allows us to set the password duration to an unlimited number of days, meaning your password will not expire or need to be reset at set intervals (there are some exceptions, listed below).

The new password policy was put in place on Monday, March 4, 2024. What you need to know:

- The next time you are prompted to reset your password, the new policy will apply.
- Your new password or passphrase must be at least 16 characters long but may be longer if you so choose.
- Your new password or passphrase does not expire or need to be changed at set intervals. There are two exceptions to the non-expiring password:
  - If your account gets compromised (your password was stolen), then you will be forced to change your password.
  - If you have access to protected information via the Secure Enclave (https://secureapps.ccsu.edu) then your password will expire every 365 days. The Microsoft Authenticator app is also required to be installed and configured as the primary authentication method for your account.

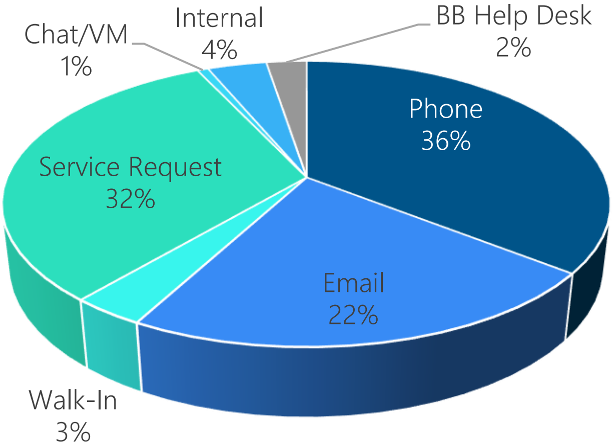
CENTRAL OFFICE OF INFORMATION TECHNOLOGY

ITC Updates

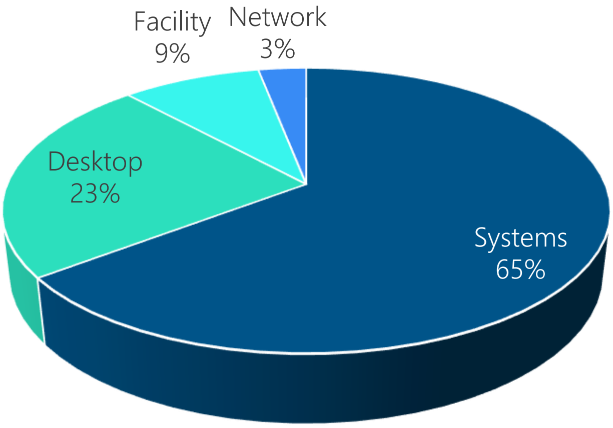
Support Statistics

January 2024 through March 2024

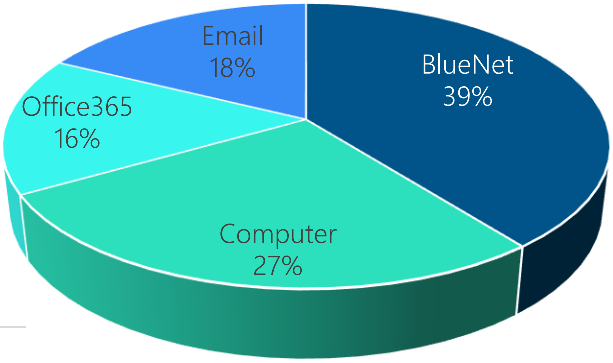
Tickets by Source



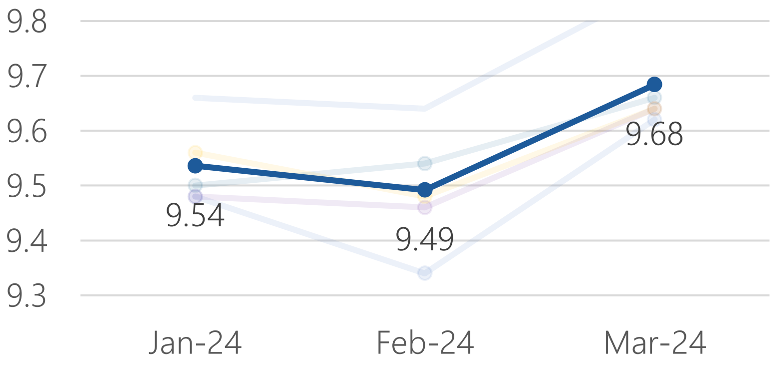
Top Incident Services



Top Incident Categories



Satisfaction Survey Average Scores



CENTRAL
OFFICE OF
INFORMATION
TECHNOLOGY

ITC Updates

Support Statistics

Tickets by Source	24-Jan	24-Feb	24-Mar	Total 3mo
Phone	1104	999	943	2103
Email	569	378	368	1315
Walk-In	84	35	78	197
Service Request	778	556	545	1879
Chat/VM	20	11	10	41
Internal	79	58	84	221
BB Help Desk	40	71	40	151
Total	**2674**	**2108**	**2068**	**6850**

Top Incident Services	24-Jan	24-Feb	24-Mar	Total 3mo
Systems	1007	855	802	2664
Desktop	379	278	311	968
Facility	137	137	89	363
Network	51	44	30	125

Top Incident Categories	24-Jan	24-Feb	24-Mar	Total 3mo
BlueNet	384	278	356	1018
Computer	268	184	253	705
Office365	137	111	156	404
Email	117	236	103	456

Customer Satisfaction	24-Jan	24-Feb	24-Mar
Analyst Courtesy	9.66	9.64	9.86
Analyst Knowledge	9.5	9.54	9.66
Overall Satisfaction	9.48	9.46	9.64
Quality of Resolution	9.56	9.48	9.64
Timeliness of Resolution	9.48	9.34	9.62
Average	**9.536**	**9.492**	**9.684**