▶ Never Change your Password Again! New Password Policy Starting March 4, 2024

To enhance account security, Central is implementing 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 will be put in place on Monday, March 4, 2024. What you need to know:

- The next time you are prompted to reset your password on or after Monday, March 4, 2024, 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.

Geofencing

Due to an uptick in malicious login attempts from outside of North America, IT is recommending we implement geofencing as a security measure to help us be more protective against these attempts. Geofencing is a location-based technology that uses GPS, cellular data, and Wi-Fi to create a virtual geographic boundary where logins are allowed. If you are traveling outside of North America and plan to use your Central account, we'll provide a short form to notify IT of your travel plans. We will then temporarily expand your geofence to allow access while you are traveling. If are not traveling or did not request for us to expand the geofence, this safeguard will automatically block any login attempts from outside of North America even if someone steals your password, thus reducing unauthorized and malicious use of your account. This change is proposed for faculty and staff accounts, with the goal of launching it by early April.
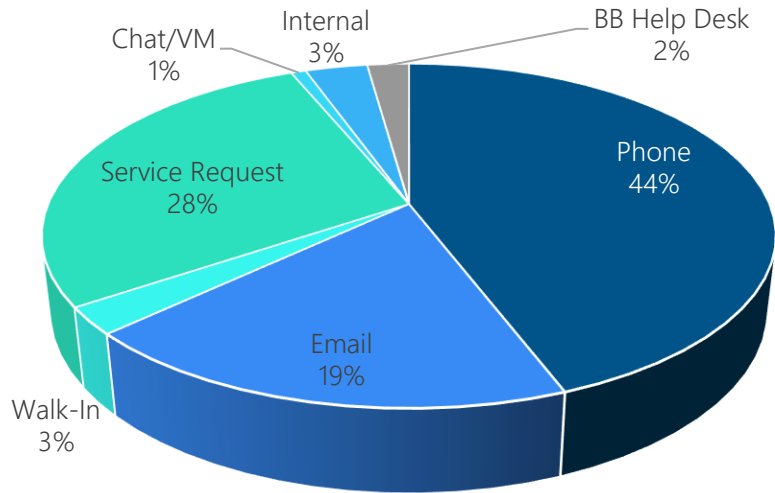
WebEx Updates

We previously announced two upcoming changes:
1. Upgrade to the WebEx administrative system to allow for single sign-on – this upgrade has been stalled because of how our licensing is connected to the BOR. We hope to have positive movement soon and will provide updates as we have them.
2. Current WebEx licensing set to expire in July of 2024 – we have had some very positive talks with Cisco and the CFO about the phone system and licensing. We may not need to change our licensing model for faculty and staff. Again, we will provide updates as we have them.
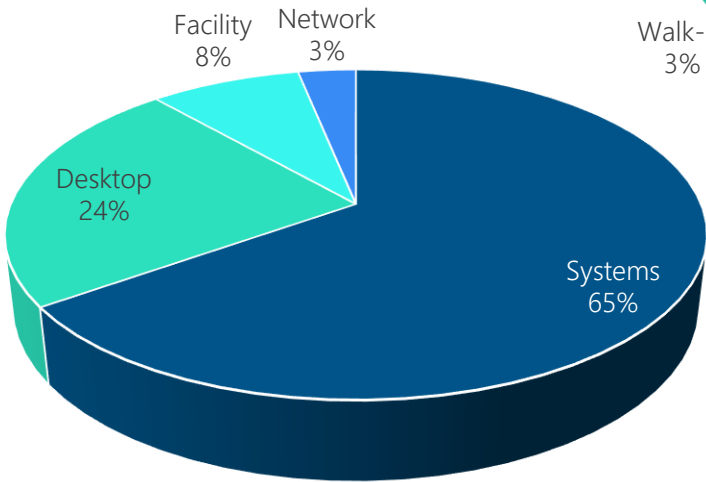
ITC Updates

Information Technology

December 2023 through February 2024

Tickets by Source

- Chat/VM 1%
- Internal 3%
- BB Help Desk 2%
- Phone 44%
- Email 19%
- Walk-In 3%
- Service Request 28%

Top Incident Services

- Facility 8%
- Network 3%
- Desktop 24%
- Systems 65%

Top Incident Categories

- Email 19%
- BlueNet 40%
- Office365 14%
- Computer 27%
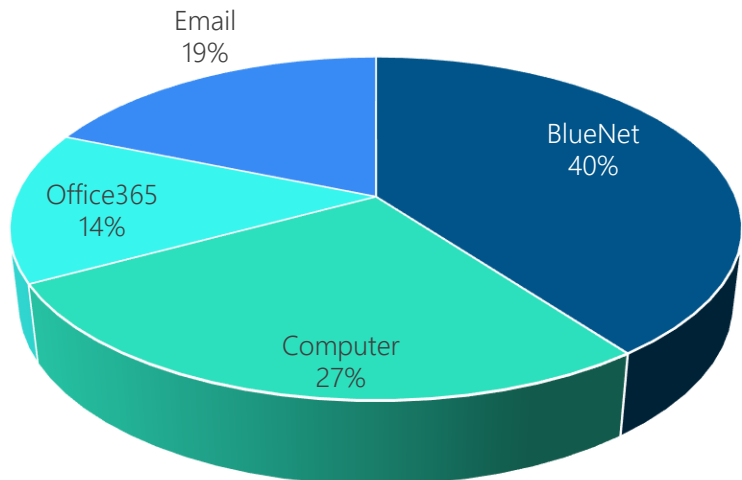
Tickets by Source	23-Dec	24-Jan	24-Feb	Total 3mo
Phone	674	1104	999	2777
Email	237	569	378	1184
Walk-In	41	84	35	160
Service Request	438	778	556	1772
Chat/VM	18	20	11	49
Internal	68	79	58	205
BB Help Desk	27	40	71	138
Total	**1503**	**2674**	**2108**	**6285**

Top Incident Services	23-Dec	24-Jan	24-Feb	Total 3mo
Systems	579	1007	855	2441
Desktop	217	379	278	874
Facility	37	137	137	311
Network	24	51	44	119

Top Incident Categories	23-Dec	24-Jan	24-Feb	Total 3mo
BlueNet	229	384	278	891
Computer	155	268	184	607
Office365	71	137	111	319
Email	65	117	236	418