Password Administration

Entering Account Security Information

When logging into your account for the first time you will be prompted to enter your security information for the first time.

Log into the system using your account information xxxxx@bryantstratton.edu

You will receive a message indicating More information required.

More information required

Your organization needs more information to keep your account secure

Use a different account

Learn more

Select Next

You will be asked to enter information to keep your account secure.

If you want to select a different authentication method select “I want to setup a different method.”
Select Email, Phone or Security questions.

Email –
Select Email then “Confirm”

Choose a different method

Which method would you like to use?

Email
Phone
Authenticator app
Security questions

Enter your personal external email address (Gmail, Outlook, Yahoo, etc.)
Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 1 of 2: Email

```
-------------------
| Email             |
| Phone             |
-------------------
```

Email

What email would you like to use?

Enter email

Select Next

Enter the code from the email you have provided then select next.

Method 1 of 2: Email

```
-------------------
| Email             |
-------------------
```

Email

We just sent a code to nw_magee@outlook.com

Enter code

Resend code

Once the code was accepted your email will be registered.
Enter your “Phone Number”

If entering your number, select either text me a code or call me then select Next.

Depending on the selection Microsoft will send you a text message with a code to validate your selection or they will call you with a code.

Once you obtain the code, please enter your code then select Next.

Once complete the authentication method will be registered successfully.
Expiring Passwords

Log into the system using your account information xxxxx@bryantstratton.edu

Enter password

Forgot my password

When the user logs into the system they will be prompted with updating their password due to a password expiration. An email should have been sent informing the user that their password was about to expire.

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

New password

Confirm password

Enter the current and new password. Once complete the password will be changed in the system.
Manually Change My Password

Log into the system and once logged in select the sprocket.

Select Change your password.

Enter the Old Password and new password information.

Once complete select Submit then relog into the system with your new password.
Forgotten Password

The following procedures are to be used when resetting a forgotten Password.

Password Reset:

Users Forgetting Passwords will need to verify their account information:

1) If a user/student forgot their password, direct them to select “Forgot my password”

2) The user/student will need to validate the captcha phrase
   a. Enter email: ex. XXX@bryantstratton.edu
   b. Enter the captcha characters
      i. Click to read out loud or reset if needed
   c. Click “Next”

3) In the “Get back into your account” users will need to select their first verification method to be used.
   a. Select one of the following options:
      i. Selecting the following will send a verification code that will need to be retrieved and entered:
         1. Email my alternate email
         2. Text my mobile phone
         3. Call my mobile phone
      ii. Retrieve and enter the verification code
         1. Click “Next”
b. Select “Answer my security questions”
   i. Answer the security questions as established prior
   ii. Click “Next”

4) Select the 2nd verification method to be used.
   a. Repeat step 3 depending on your selection:

   **NOTE:** if you are having issues select Contact your administrator and it will navigate to the Blackboard support center.

5) Once verification is complete users/students will be able to enter a new password.
   a. Enter new password:
      i. Look for the indicator to show “Strong”
   b. Enter new password again to confirm
   c. Click “Finish”

6) Select “click here” to sign in with your new password.
IF forgot password reset information, please follow the below ---

**End Users/Students**: The Below steps need to be processed by the end user/student if they had forgotten their password reset information.

Once the student / user can log into their device they will need to be directed in resetting there self-service password reset (SSPR) and update their contact information under Security Info.

1. Navigate to the *security information* page located in Microsoft 365, by using the following methods:
   a. Use this link to navigate to the security information →
      [https://mysignins.microsoft.com/security-info](https://mysignins.microsoft.com/security-info)
   b. If connecting to security information manually have the user log in and select the user’s profile by selecting “View Account”.
   c. Once logged in select “Security Info”

2. The student can *change* and or *add* the sign-in methods from this menu by selecting “Add sign-in method”

3. From the drop down the user can then add the method
   a. Complete the required information based upon the selection

4. If removing method, the user can select “Delete” on a method then add their sign-in methods again.
FAQ Information:

We recommend all users create a **passphrase** instead of just a password. For example, the passphrase "My-passw0rd-is-Super-str0ng!" is 28 characters long and includes alphabetic, numeric and special characters.

Passphrase complexity requirements are as follows:

- At least passphrase **14 characters in length**;
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z);
- Have at least one numerical character (e.g. 0-9) and
- Have at least one special character (e.g. ~!@#$%^&[]{}*()-_+=).

Your passphrase should **NOT**:

- Spell a word or series of words that can be found in a standard dictionary regardless of language;
- Spell a word with a number added to the beginning and the end;
- Be based on any personal information such as BID, family name, pet, birthday, etc.;
- Be similar to a password you have used in the past or that you are using with other accounts (even personal ones).

Here are some recommendations for maintaining a strong passphrase:

- Do not share your passphrase with anyone for any reason, even with IT as we can reset your password;
- Change your passphrase upon any indication of compromise;
- Do not write your passphrase down or store it in an insecure manner;
- Avoid reusing a passphrase;
- Consider surrounding your passphrase with a [ ]?..example: [My-passw0rd-is--str0ng!];
- Avoid using the same passphrase for multiple accounts;
- Do not use automatic logon functionality.

When in doubt, test your passphrase schema at [https://www.passwordmonster.com](https://www.passwordmonster.com).

Q. How often do passwords expire?

Passwords expire every 180 days, and an expiration email should be sent out informing the user of that change with detailed instructions.

Q. If I forget my password, and I've setup my recovery questions, what do I need to do?

Please follow the forgotten password step as this step will help change your current password.

Q. If my password has expired and I am receiving the message "authentication failed" when I try to login to IOffice365, Banner SSB, or Blackboard, what do I need to do?

Please follow the expiring password section of this documentation as this will help you change your password.
Q. Will I receive any notice that my password has expired?
Yes, notification will be sent via email in relation to expiring passwords please follow the directions within that email. If your password has expired and was forced changed please follow the forgotten password.

Q. How will I know the notification is legitimate and not a phishing scam?
All email correspondences in relation to password expirations should come from the following address.

bscnoreplycredential@bryantstratton.edu

Q. Are there any requirements for passwords?

Things to consider:
Don’t reuse the same password for multiple sites
Don’t set an impossible-to-memorize passwords
Don’t store passwords in places that aren’t secure