ASPEN SNOWMASS

MULTIFACTOR AUTHENTICATION FACT SHEET

WHAT IS MULTIFACTOR AUTHENTICATION?

Almost all online services - banks, social media, and shopping sites-- have added a way for your accounts to be more secure. You may hear it called "Two-Step Verification" or "Multifactor Authentication." Either way, it's the same principle: When you sign into the account for the first time on a new device (like a cell phone or computer) or application (like the employee portal or Kronos) you need more than just the username and password. A password alone is not sufficient security nowadays. Your data can still be hacked and phished. You need a second "factor" to prove who you are. Once a system recognizes your device, you should not have to provide a second factor again when you log in. You will only be prompted for the second factor authentication on a new device or the first time a new ASC application is moved to multifactor authentication.

The extra security comes from the fact that someone trying to break into your account is probably not also doing so on another device so they'll need to have that second factor to get in. If somebody tries to sign in as you, they'll enter your username and password, and when they get prompted for that second factor from another device they're stuck.

WHAT DO I HAVE TO DO TO SET THIS UP?

It is a short process that should only take a few minutes. On February 23, the Employee portal was enabled for multi-factor authentication. On March 17 Empyrean was enabled. On April 20, Kronos will be enabled. When you go to the website, click the sign in link and follow the steps. MFA Set-Up Directions are here if you need them. If you prefer to receive authentication via text, you can preview a how-to video here. If you would like to use the mobile phone app, a helpful video to preview is here.

DO I HAVE TO DO THIS? I'M A SEASONAL EMPLOYEE.

Aspen Skiing Company takes the confidentially of your personal information seriously. This is an important step we need to take as a company to protect your personal information, such as Social Security Number and Direct Deposit details. You also will not be able to access ASC applications including the employee portal (after Feb. 23), Empyrean (after March 17), and Kronos (after April 20), and Smart Recruiter when they switch to requiring MFA.

WHAT HAPPENS WHEN I LEAVE AT THE END OF THE SEASON AND COME BACK IN THE FALL?

You may have to re-enroll upon returning next season. If you're planning to come back in the fall, we'll have more information then.

IS MY DATA COMPLETELY SAFE NOW?

We're never 100% safe, but this move ensures that we are using the same type of safety protocol as banks and other businesses that protect your data.

ASPEN SNOWMASS

WHAT IF I DON'T HAVE A CELL PHONE?

You can also use your office phone or a landline home phone or come in to HR. Just be aware that when you need to authenticate a new device or application, you will need to be near that phone to answer it and receive the authentication. If you have additional questions, we recommend calling IT Support to discuss your options.

WHAT HAPPENS IF I DON'T DO THIS?

We think it's incredibly important to go through this short process to protect your personal and online data. If you choose not to, you eventually will not be able to access any ASC applications and your data will be at elevated risk.

WHAT IF I LATER WANT TO CHANGE HOW I AUTHENTICATE (for instance, I've changed my phone number)

To change your authentication delivery information or modify your Microsoft Multi-factor settings, please visit aka.ms/MFASetup. Also, if you're changing offices or jobs at ASC, reach out to the IT Support Desk for assistance.

ARE WE DOING THIS FOR PROCARD AS WELL?

Not at this time. The only applications that will be impacted by this change are: Employee Portal, Empyrean (Employee Benefits), UKG Kronos, and Smart Recruiters.

WHAT ELSE SHOULD I KNOW?

- Once an employee goes through this full authentication enrollment process, they should not have to repeat this process when other applications are rolled over to MFA. As each new ASC application is brought online, they will have to authenticate on their device (meaning they'll be asked for that extra factor). After that, it should work as normal.
- Employees will be asked to authenticate once per application and/or per device every 90 days if they have been idle.
- Employees should choose carefully where they want their authentication notifications to go to before they begin the process of enrolling. For instance, if they choose their office phone to receive a notification and they're working from home, they won't be able to access the code they need to get into the application.
- If an employee is using a computer shared by many, they should log off from the application each time they are finished. They will have to authenticate each time they log in to an application on a shared computer as well.

WHAT'S NEXT AFTER I DO THIS?

Once you enroll and authenticate your devices, you should not have to do anything else additional for now unless you are authenticating a new device or using a shared computer (where you will authenticate each time). When the next ASC application moves to multifactor authentication, we will notify you by email. The first time you log in to this application after this date you will be required to authenticate on each device when you try to log in.

I CAN'T FIGURE THIS OUT—WHO DO I GO TO FOR HELP?

Our IT Department is standing by to help you if you need support and assistance. Hours are 8am-5pm.

- Mountain Help Desk: itsupport@aspensnowmass.com, 970-300-7070
- Hotel Help Desk: hotelit@aspensnowmass.com, 970-920-6396