Hisense Gorenje Europe, d.o.o.
IT department

Introduction to Multifactor Authentication

In the computer security world, there is an ongoing silent war between those who want to gain unauthorised access to our data and those of us who want to prevent them from doing so.

Attacks, especially phishing attacks, that try to steal user's login information are getting increasingly common, more sophisticated, and unfortunately, also more successful.

Therefore, to provide better data security we use:

- Secure sign-in to Office 365 services
- Securing the data on mobile devices
- Hard disk encryption for laptops and notebooks

1 Secure Sign-in to Office 365 Services

To enhance the security of sign-in to Office 365 services, we have introduced multifactor authentication.

Multifactor Authentication (hereinafter: **MFA**) is additional verification of your identity that is above the usual use of username and password.

By employing these tools, the phishing attacks that we witnessed in the past should be much more limited and, in most cases, even prevented.

After your MFA service is activated, we recommend visiting the web page https://portal.office.com. Sign in with your AD username. If you are signing in from the company's internal network, you will not need to enter the password. After that, the system will ask you to setup your MFA.

End users will have to specify which means of additional authentication they want to use. Available options are:

- Sending a text message (SMS) to a selected mobile number
- Automated call to selected phone number (the call is in your local language)
- Mobile application – authenticator

Each user can select any combination of one or more options listed above and specify which one of them will be primarily used for signing in.

If at the given moment the selected sign-in method does not work, you will be able to select from any other previously specified sign-in methods.

From now on, the system will ask you to confirm your identity by using MFA every time you try to sign in to Office 365 services (e.g. Outlook, Skype for Business, SharePoint Online and others).

When you have signed in, you can use Office Portal to manage your MFA settings, add or remove sign-in methods or modify stored phone numbers.

The stored phone numbers can also include your landline office phone number as specified by system administrators. It is the only phone number that you cannot modify by yourself; if you find it unsuitable, please contact IT Helpdesk.

Important: sign-in without MFA will no longer be possible.

After MFA is activated, the access to e-mail on mobile devices will only be possible via Intune MAM.

1.1 Who Can See Your MFA Data

The data entered by users for MFA purposes is only visible to the Microsoft Corporation as the owner and manager of Office 365 services; they undertake to use this data solely for MFA purposes.

System administrators from Hisense Gorenje cannot see the phone numbers set by the users for MFA purposes. In case of sign-in problems, system administrators can only delete your current MFA settings - in such case, you will have to repeat the MFA configuration.

Before entering any phone numbers for MFA purposes, we recommend reading the general terms and conditions available on the MFA setup website.

1.2 MFA Methods

1.2.1 SMS

A text message (SMS) is probably the simplest way to use MFA.

When singing in, you will receive a text message with a 6-digit numeric code which you will enter in the sign-in field.

The text message is valid for a few minutes; after that, you will have to repeat the sign-in attempt and receive a new message with a new code.

You can receive these text messages on your company-assigned or privately owned mobile phone; however, you cannot receive them on landline phones.

To receive text messages, you do not have to install any applications or use a smartphone or enable mobile data (which is very important while roaming).

If your phone breaks down, you can receive text messages on another phone by transferring your SIM card.

When using SMS for MFA, please keep in mind that SMS delivery depends on your mobile operator and text messages can be delivered with substantial time delay. Therefore, the sign-in process may have to be repeated or you may need to select an alternative MFA method (e.g. a phone call).

Important: if you start receiving text messages with sign-in codes without triggering the sign-in process yourself, this means that somebody else is using your username and password to sign in. In such case, change your password immediately and notify the IT Helpdesk.

1.2.2 Phone Call

When using phone call for MFA, the automated call system calls your selected phone number. The phone call is in your language even when the calling number is from another country.

During the phone call, the system asks you to confirm the sign-in by pressing the # sign (hash) and allows you to directly report any attempts of unauthorised sign-in.

The phone call is free of charge, except if you are called on a mobile phone while roaming.

If you receive MFA calls on your office phone that is a part of the local phone switchboard, please contact your IT support about the use of phone keyboard for tone dialling during the call.

On the Alcatel switchboard which is used in Hisense Gorenje in Velenje and Šoštanj, tone dialling must be enabled during the call. Tone dialling is enabled by pressing the keys # (hash) and 0 (zero). The full confirmation sequence on Alcatel switchboard is therefore # 0 #.

If you are confirming sign-in on your home phone, the #-key (hash) will probably be enabled; if not, consult your phone's user manual.

If your only MFA method is a call to your office phone, please keep in mind you will not be able to use Office 365 services outside your office.

Important: if you start receiving calls for sing-in confirmation without triggering the sign-in process yourself, this means that somebody else is using your username and password to sign in. In such case, do not confirm the sign-in. If you are the only user of this phone number, change your password immediately and notify the IT Helpdesk.

If your confirmation phone number is used by multiple users, never confirm any sign-in requests that you have not triggered yourself.

False confirmation of sign-ins stipulates a serious violation of working obligations.

1.2.3 Mobile Application

Mobile application **Microsoft Authenticator** works in two ways:

- It generates a 6-digit code that is recreated every 30 seconds
  The code can be used in a similar way as the SMS messages but does not require receiving an SMS message - this is very useful if you are working in an area without mobile coverage.
- It allows you to confirm or deny the sign-in by pressing the buttons Confirm / Deny.
  In such case, the request for confirmation is displayed as a notification on the phone.

For initial configuration, the application requires mobile data and access to the phone's camera, because it must read a QR code from your computer's screen to connect the locally installed application and your user account in the Office Portal.

We recommend installing the Microsoft Authenticator application only via the Intune Company Portal; only then we can ensure that this is the original application published by Microsoft and confirmed by Hisense Gorenje IT.

Frequent questions and answers regarding the application can be found at:
https://docs.microsoft.com/en-us/azure/multi-factor-authentication/end-user/microsoft-authenticator-app-faq

Important: if the application starts asking you for sing-in confirmation without triggering the sign-in process yourself, this means that somebody else is using your username and password to sign in. In such case, do not confirm the sign-in; instead, change your password immediately and notify the IT Helpdesk.

2 Securing the Data on Mobile Devices

If until now you have used a mobile device (company-assigned or your own) to access company e-mail, you might be aware that system administrators can trigger remote wipe of the entire device. In such case, all the data in the internal storage of the phone was deleted, including your private photos, music, applications, etc.

Intune Mobile Application Management (Intune MAM) encloses work-related data on your mobile device (phones and tablets with iOS or Android) in their own encrypted storage space (container) that is separated from other contents on the device.

On one hand, this prevents various malware applications from accessing the work-related data. On the other hand, this enables system administrators to selectively erase just the work-related data (contents of the container) from your mobile device without affecting your personal data.

Intune MAM can be used both on company-assigned and privately owned mobile devices. In the future, accessing the work-related data on mobile devices will no longer be possible without using Intune MAM.

2.1 Intune Company Portal Application

When administrators activate your Intune MAM access, your e-mail access via your current mobile applications (e.g. default applications on mobile devices) will stop working and you will receive a notification to install the Intune Company Portal application on your mobile device - the notification includes the installation link for your official application store (AppStore for iOS or PlayStore for Android).

If you wish to start using your mobile device to access work-related data, but you have not used it to access the company e-mail before, contact the IT Helpdesk; they will enable the use of advanced security solutions for you. Only then install the **Intune Company Portal** to your mobile device. Be careful to install the application from the official application store (AppStore for iOS or PlayStore for Android). Please make sure that **Microsoft Corporation** is indicated as the publisher of the application.

After the installation, the Intune Company Portal requires mobile device locking to be enabled (by PIN, password or fingerprint).

You will have to sign in to the Intune Company Portal with your company credentials; after that, an encrypted container will be created and the Intune Company Portal will offer you installation of other applications like Outlook, Authenticator, Skype for Business, Word, Excel and others.

Important: when using your mobile device, if you get a notification asking you to install some application that is not published in the Intune Company Portal, it is very likely a phishing attempt. We recommend you not to install the mentioned application. If you are in doubt, please contact the IT Helpdesk

For business needs, please install only the applications published in the Intune Company Portal.

The Intune Company Portal provides single sign-on to other published applications and normal data exchange between these applications, while other applications cannot access the internal information.

If you have previously used Outlook mobile application for e-mail, uninstall it and reinstall it via the Intune Company Portal.

If you have used a third-party application for mobile access to the company e-mail, remove the configured Exchange account from that application after installing the Intune Company Portal and Outlook. This will free up a lot of storage space on your mobile device and it will prevent you from leaving any old work-related data unprotected on the device.

We recommend that you enable contacts synchronisation in your account’s settings in the Outlook application - this will enable other applications on the phone to access your Outlook contacts.

3 Hard Disk Encryption for Laptops and Notebooks

Hard disk encryption prevents access to locally stored data in case the computer is stolen.

The hard disk is encrypted by **BitLocker** which is a part of the Windows operating system.

Encryption keys are stored in the special chip in the laptop (Trusted Platform Module, TPM); they are locked with PIN code. Upon booting, the user must enter the PIN code and only after that the system can start up normally.

You also have to enter the PIN every time the computer is recovering from sleep mode; however, entering the PIN is not required for every unlocking of the computer.

When you finish working on the computer, briefly press the power key - the computer will enter the sleep mode and erase the encryption keys from the memory. Thus, you have protected the contents of the hard disk.

To activate BitLocker on your laptop, please contact the IT Helpdesk. The duration of initial hard disk encryption depends on the amount of data and the speed of disk; it usually takes approximately 30 minutes.

4 Final thoughts

The Hisense Gorenje IT department makes strong efforts to provide you, our users, with secure, reliable and simple means of accessing the work-related data, regardless the location from which you attempt to access them and the device used for that purpose.

In the future, you can expect further similar services; they will all be related to the solutions presented in this document.

We wish you successful and safe work.
Your Hisense Gorenje IT Department