



PEMERINTAH KABUPATEN NIAS

Gido, 27 Maret 2025.

Nomor : 800.1.13/0956/BKPSDM/III/2025
Sifat : Penting
Lampiran : 1 (satu) set
Hal : Penerapan *Multi-Factor Authentication*
(MFA)

- Sdr. 1. Sekretaris Daerah Kabupaten Nias
2. Staf Ahli Bupati Nias
3. Asisten Sekda Kabupaten Nias
4. Kepala Perangkat Daerah/Unit Kerja Lingkup
Pemerintah Kabupaten Nias
5. Camat Lingkup Pemerintah Kabupaten Nias
6. Kabag Lingkup Setda Kab. Nias

di
Tempat

Untuk: _____

Sehubungan dengan surat Deputi Bidang Sistem Informasi dan Digitalisasi Manajemen Aparatur Sipil Negara Nomor 2960/B-SI.02.01/SD/E/2025 tanggal 19 Maret 2025 Hal Penerapan *Multi-Factor Authentication* (MFA), dengan ini disampaikan hal-hal sebagai berikut:

1. Bahwa seiring dengan meningkatnya ancaman siber yang semakin canggih, seperti phishing, pencurian identitas, dan peretasan akun, kebocoran data bisa berdampak luas terhadap keamanan serta kepercayaan publik. Sehingga, diperlukan upaya strategis untuk memperkuat perlindungan data kepegawaian termasuk perlindungan data pribadi ASN.
2. Bahwa beberapa faktor utama yang menyebabkan kebocoran data adalah penggunaan kredensial yang lemah, kerentanan sistem, dan adanya malware Stealer (pencuri kredensial) pada perangkat/gawai sehingga diperlukan langkah-langkah efektif untuk meningkatkan keamanan layanan digital, salah satunya melalui penerapan Multi-Factor Authentication (MFA). Dengan MFA, autentikasi tidak hanya mengandalkan password, tetapi juga beberapa faktor tambahan seperti OTP (One-Time Password), sehingga memperkecil peluang peretas dalam menyusup ke sistem.
3. Bahwa untuk kelancaran penerapan MFA diperlukan langkah-langkah sebagai berikut:
 - a. Penerapan *single access* login melalui platform ASN Digital dengan tautan <https://asndigital.bkn.go.id> memudahkan ASN mengakses seluruh layanan Manajemen ASN BKN dengan satu kali login, tanpa perlu membuka banyak tautan.

- b. **Seluruh ASN wajib melakukan aktivasi MFA melalui platform ASN Digital.** Tata cara aktivasi MFA dapat dilihat pada tautan berikut: s.id/aktivasiimfaasn
 - c. Akses langsung ke tautan setiap layanan akan ditutup dan dialihkan ke platform ASN Digital **mulai tanggal 23 Maret 2025 pukul 23:59 WIB.**
 - d. Untuk kebutuhan notifikasi layanan, diperlukan data nomor telepon dan email. Pastikan data tersebut telah sesuai/update pada profil ASN. Jika data belum sesuai/update silahkan segera melakukan pemutakhiran melalui fitur Update Data Mandiri pada MyASN serta layanan Peremajaan Data bagi pengelola kepegawaian yang memiliki kewenangan.
 - e. Jika menemukan kendala dalam pemanfaatan MFA, dapat disampaikan melalui layanan Helpdesk pada platform ASN Digital dengan cara pilih menu Layanan Pendukung kemudian pilih Layanan Helpdesk.
4. Selain menerapkan MFA, seluruh ASN dihimbau agar menggunakan password yang kuat dan unik untuk setiap akun, mengganti password secara berkala, serta tidak membagikan password ke pihak lain.

Demikian disampaikan, atas perhatian diucapkan terima kasih.

a.n. BUPATI NIAS
SEKRETARIS DAERAH,

SAMSON P. ZAI, S.H., M.H.

Tembusan Yth:

Kepala Kantor Regional VI Badan Kepegawaian Negara



BADAN KEPEGAWAIAN NEGARA

Jalan Mayor Jenderal Sutoyo Nomor 12 Cililitan, Kramat Jati, Jakarta Timur 13640
Telepon (021) 8093008; Faksimile (021) 8090421
Laman: www.bkn.go.id; Pos-el: humas@bkn.go.id

Jakarta, 19 Maret 2025

Nomor : 2960/B-SI.02.01/SD/E/2025
Sifat : Penting
Lampiran : -
Hal : Penerapan *Multi-Factor Authentication* (MFA)

Yth. 1. Kepala Biro Kepegawaian/SDM Instansi Pusat
2. Kepala BKD/BKPSDM/BKPP Instansi Daerah
di
tempat

Seiring dengan meningkatnya ancaman siber yang semakin canggih, seperti *phishing*, pencurian identitas, dan peretasan akun, kebocoran data bisa berdampak luas terhadap keamanan serta kepercayaan publik. Sehingga, diperlukan upaya strategis untuk memperkuat perlindungan data kepegawaian termasuk perlindungan data pribadi ASN. BKN terus berupaya melakukan antisipasi terhadap kebocoran dan penyalahgunaan data serta memastikan layanan berbasis digital tetap aman, andal, dan dapat diakses dengan mudah oleh seluruh ASN.

Beberapa faktor utama yang menyebabkan kebocoran data adalah penggunaan kredensial yang lemah, kerentanan sistem, dan adanya *malware Stealer* (pencuri kredensial) pada perangkat/gawai sehingga diperlukan langkah-langkah efektif untuk meningkatkan keamanan layanan digital, salah satunya melalui penerapan *Multi-Factor Authentication* (MFA). Dengan MFA, autentikasi tidak hanya mengandalkan *password*, tetapi juga beberapa faktor tambahan seperti OTP (*One-Time Password*), sehingga memperkecil peluang peretas dalam menyusup ke sistem.

Perlu kami informasikan, bahwa untuk kelancaran penerapan MFA diperlukan langkah-langkah sebagai berikut:

1. Penerapan *single access login* melalui platform ASN Digital dengan tautan <https://asndigital.bkn.go.id> memudahkan ASN mengakses seluruh layanan Manajemen ASN BKN dengan satu kali login, tanpa perlu membuka banyak tautan.

2. Seluruh ASN wajib melakukan aktivasi MFA melalui platform ASN Digital. Tata cara aktivasi MFA dapat dilihat pada tautan berikut: s.id/aktivasiimfaasn
3. BKN telah melakukan sosialisasi teknis secara nasional pada tanggal 17 Maret 2025 melalui Zoom *meeting* serta Youtube *channel* resmi BKN dengan peserta seluruh unit pengelola kepegawaian instansi beserta para ASN. Selanjutnya BKN Pusat termasuk Kantor Regional I s.d. XIV bersama dengan Biro SDM/Biro Kepegawaian Instansi Pusat, BKD/BKPP/BKPSDM Instansi Daerah melakukan pendampingan lanjutan kepada seluruh ASN.
4. Akses langsung ke tautan setiap layanan akan ditutup dan dialihkan ke *platform* ASN Digital mulai tanggal 23 Maret 2025 pukul 23:59 WIB.
5. Untuk kebutuhan notifikasi layanan, diperlukan data nomor telepon dan *email*. Pastikan data tersebut telah sesuai/update pada profil ASN. Jika data belum sesuai/update silahkan segera melakukan pemutakhiran melalui fitur *Update* Data Mandiri pada MyASN serta layanan Peremajaan Data bagi pengelola kepegawaian yang memiliki kewenangan.
6. Jika menemukan kendala dalam pemanfaatan MFA, dapat disampaikan melalui layanan *Helpdesk* pada *platform* ASN Digital dengan cara pilih menu Layanan Pendukung kemudian pilih Layanan *Helpdesk* atau dapat menghubungi Kantor Regional BKN setempat.

Selain menerapkan MFA, BKN juga menghimbau kepada seluruh ASN agar menggunakan *password* yang kuat dan unik untuk setiap akun, mengganti *password* secara berkala, serta tidak membagikan *password* ke pihak lain.

Penerapan MFA dan integrasi layanan kepegawaian pada platform ASN Digital diharapkan meningkatkan keamanan dan efisiensi. BKN berkomitmen mendukung transformasi digital dan penguatan keamanan informasi ASN.

Demikian disampaikan, atas perhatian dan kerja samanya diucapkan terima kasih.

Deputi Bidang Sistem Informasi dan Digitalisasi
Manajemen Aparatur Sipil Negara

Ditandatangani Secara Elektronik



Suharmen, S.Kom., M.Si
NIP. 196702271990031002



Tembusan :
Kepala Badan Kepegawaian Negara, sebagai laporan;

Aktivasi Multi-Factor Authentication (MFA) SSO BKN



Download Authenticator



Google Authenticator

Google LLC

4.3★
224K reviews

100M+
Downloads

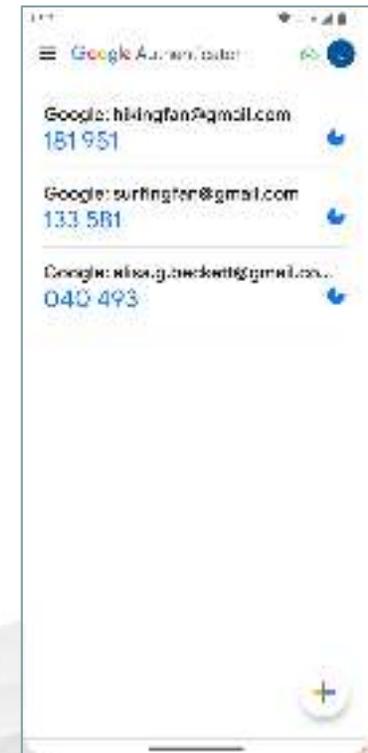
13+
Rated for 13+

Install

Share

Add to wishlist

This app is available for all of your devices.



Masuk di layanan BKN



ASN Karier

SIASN



login menggunakan SSO



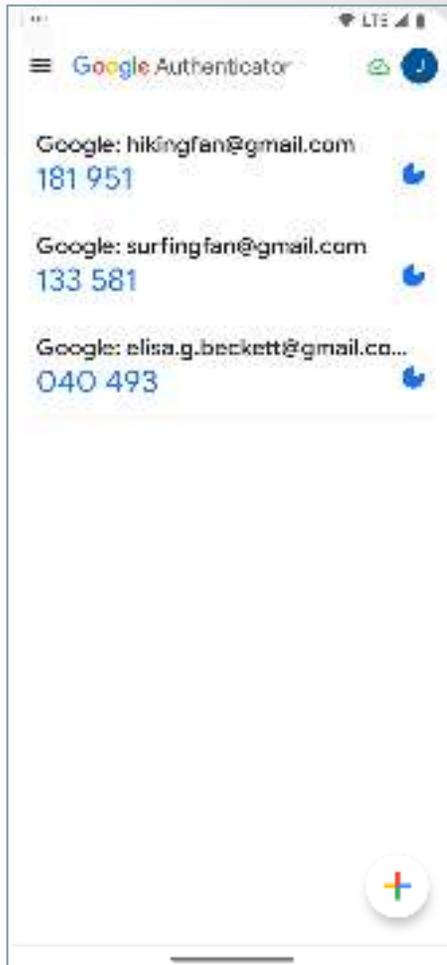
**Masukkan
username dan password**

**Kemudian tampil
permintaan daftar Authenticator**



Scan Barcode

Scan barcode menggunakan Google Authenticator



2. Open the application and scan the barcode:



[Unable to scan?](#)



Masukkan code dari Aunthenticator

**Masukkan
code dalam Aunthenticator
serta Nama Perangkat**

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

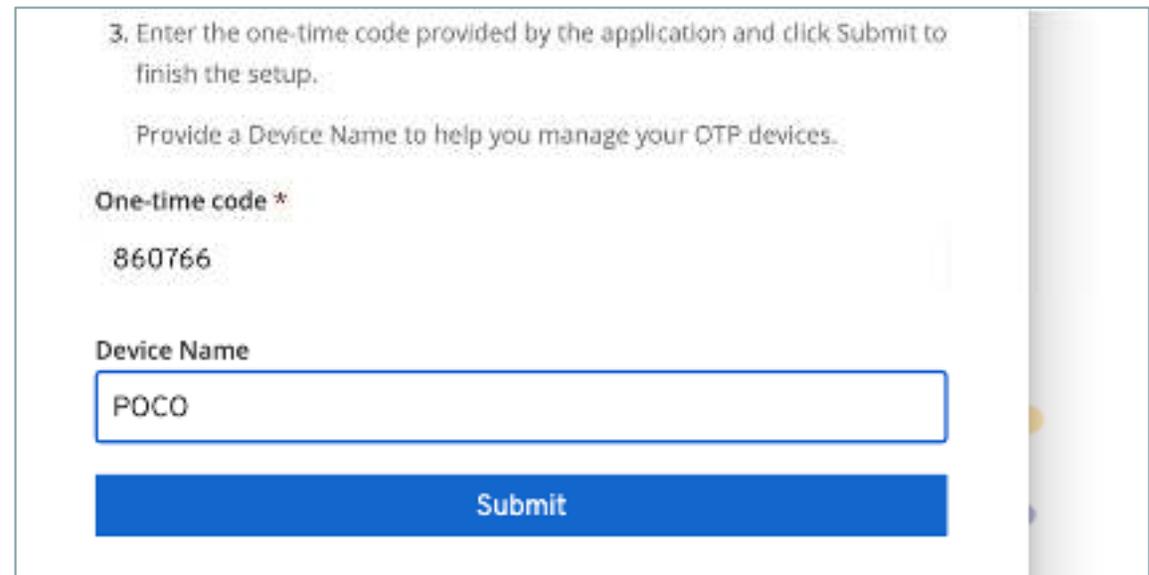
One-time code *

860766

Device Name

POCO

Submit

A screenshot of a web-based authentication setup interface. It features a blue header bar with the title 'Masukkan code dari Aunthenticator'. Below the header, on the left, is a bold black text instruction: 'Masukkan code dalam Aunthenticator serta Nama Perangkat'. On the right, a white rectangular box contains the setup steps. Step 3 instructs the user to enter a one-time code and click 'Submit'. Below this, there is a prompt to provide a device name. A text input field for the one-time code contains the value '860766'. Another text input field for the device name contains the value 'POCO'. A blue 'Submit' button is positioned at the bottom of the form. The background of the slide shows a blurred image of a group of business people holding hands.

Berhasil Login

