



PEMBERITAHUAN PENTING!



LAKUKAN PERGANTIAN PASSWORD AKUN EMAIL KEMENDAG

Demi menjaga keamanan akun dan data, seluruh pengguna **wajib** melakukan pergantian password melalui:



LOGIN SEKARANG DI

webmail.kemendag.go.id

MENGAPA PERGANTIAN PASSWORD PENTING?



MENJAGA KEAMANAN AKUN ANDA

Mencegah penyalahgunaan akun oleh pihak yang tidak berwenang.



MENCEGAH AKSES TIDAK SAH

Melindungi akun dari percobaan peretasan dan akses ilegal.



MELINDUNGI DATA DAN INFORMASI

Menjaga kerahasiaan data dan informasi Kementerian Perdagangan.



BATAS WAKTU PERGANTIAN PASSWORD



31 JULY 2026



Jika hingga batas waktu tersebut password **BELUM** diganti, maka Anda **TIDAK AKAN DAPAT LOGIN** ke akun email Anda.

AKIBAT JIKA TIDAK MELAKUKAN PERGANTIAN PASSWORD



- ✗ Akun email Anda tidak dapat diakses.
- ✗ Anda tidak dapat mengirim maupun menerima email.
- ✗ Akses ke layanan internal Kementerian lainnya mungkin terdampak.
- ✗ Proses pemulihan akun akan membutuhkan waktu lebih lama.

LANGKAH-LANGKAH PERGANTIAN PASSWORD



BUTUH BANTUAN?



Jika Anda mengalami kendala atau membutuhkan bantuan terkait pergantian password, silakan buat tiket melalui aplikasi **HERO**.
Tim PDSI akan siap membantu Anda.



Mari bersama-sama menjaga keamanan akun dan data Kementerian Perdagangan.
Ganti password sekarang, kerja lebih aman, data lebih terjaga!



Terima kasih atas perhatian dan kerja samanya!



JAGA DATA, JAGA KERJA KITA

DATA AMAN, KERJA NYAMAN

Keamanan informasi adalah tanggung jawab kita bersama.
Setiap data yang kita kelola adalah aset Kementerian Perdagangan.
Lindungi data, lindungi layanan, wujudkan Kemendag yang andal dan terpercaya.

10 PRAKTIK KEAMANAN DATA DI LINGKUNGAN KANTOR SESUAI ISO/IEC 27001:2022

1 LINDUNGI AKSES KE DATA



- Gunakan password kuat dan unik.
- Jangan bagikan password, PIN, atau OTP.
- Aktifkan MFA jika tersedia.
- Kunci komputer (Lock Screen) saat meninggalkan meja.

ACCESS CONTROL & AUTHENTICATION

2 SIMPAN DATA PADA MEDIA RESMI



- Simpan dokumen pada File Server, NAS, Share Folder, atau media resmi lainnya.
- Pastikan data penting telah masuk dalam mekanisme backup.

INFORMATION STORAGE

3 JANGAN GUNAKAN MEDIA PRIBADI



- Jangan gunakan flashdisk pribadi, hard disk eksternal, atau cloud pribadi (Google Drive, Dropbox, OneDrive, dll) untuk data kedinasan.
- Hanya gunakan media yang telah disetujui.

USE OF INFORMATION & ASSETS

4 AKTIFKAN LOCK SCREEN SAAT MENINGGALKAN KOMPUTER



- Aktifkan Lock Screen setiap meninggalkan komputer, meskipun hanya sebentar.
- Ini mencegah akses tidak sah terhadap data Anda.

PHYSICAL SECURITY

5 WASPADAI EMAIL PHISHING



- Periksa alamat pengirim.
- Jangan membuka lampiran atau klik tautan mencurigakan.
- Laporkan email mencurigakan ke HERO.

SECURITY AWARENESS

6 INSTAL APLIKASI SESUAI KETENTUAN



- Instal software hanya untuk kebutuhan pekerjaan.
- Gunakan aplikasi berlisensi.
- Jangan instal aplikasi tanpa persetujuan.

CONFIGURATION MANAGEMENT

7 LINDUNGI DOKUMEN FISIK



- Jangan tinggalkan dokumen penting di meja.
- Simpan dokumen rahasia di lemari terkunci.
- Hancurkan dokumen yang sudah tidak digunakan.

PHYSICAL SECURITY

8 TERAPKAN CLEAN DESK & CLEAR SCREEN



- Kunci komputer.
- Tutup aplikasi yang memuat data sensitif.
- Simpan dokumen penting.
- Jangan tinggalkan password tertulis di meja.

PHYSICAL SECURITY

9 GUNAKAN PERANGKAT RESMI



- Gunakan laptop/komputer kantor.
- Jangan memindahkan data ke perangkat pribadi.
- Jangan hubungkan perangkat tidak dikenal ke komputer kantor.

ASSET MANAGEMENT

10 PASTIKAN DATA TELAH DI-BACKUP



- Pastikan data kerja tersimpan pada lokasi yang di-backup.
- Data dapat dipulihkan.
- Jangan hanya simpan data di laptop Anda.

BACKUP



Jika menemukan celah keamanan atau insiden siber, atau kendala layanan TIK bisa melaporkan pada Layanan Help and Resolve HERO



Menerima email phishing



Password diketahui orang lain



Komputer terindikasi virus



File tiba-tiba terenkripsi



Menemukan akses tidak sah ke akun/aplikasi