PEMERINTAH KABUPATEN KUTAI TIMUR
Dinas Komunikasi, Informatika, Statistik dan Persandian
Tim Tanggap Insiden Siber — KUTIM-CSIRT

PANDUAN TEKNIS

Tata Kelola Kata Sandi dan Autentikasi

Acuan praktis pengelolaan kata sandi dan autentikasi yang aman bagi pegawai di lingkungan Pemerintah Kabupaten Kutai Timur.

Nomor Dokumen	**KUTIM-CSIRT/PANDUAN/003/2026**
Versi	**1.0**
Klasifikasi	**TERBUKA — untuk umum**
Tanggal Terbit	**Mei 2026**
Disusun oleh	**Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT)**

KUTIM-CSIRT
csirt.kutaitimurkab.go.id · csirt@kutaitimurkab.go.id

Kata Pengantar

Akun pengguna dan kata sandi adalah kunci utama yang membuka akses ke sistem informasi pemerintahan. Selama kunci itu terjaga, sebagian besar data dan layanan tetap aman. Sebaliknya, satu kata sandi yang lemah atau bocor sudah cukup untuk membuka jalan masuk bagi pihak yang tidak berhak.

Penanganan insiden di lingkungan Pemerintah Kabupaten Kutai Timur menunjukkan bahwa penyalahgunaan akun adalah penyebab gangguan keamanan yang paling sering ditemukan. Akun dengan kata sandi yang mudah ditebak, dipakai berulang di banyak layanan, atau tidak pernah diganti menjadi titik lemah yang dimanfaatkan untuk perusakan, penyisipan konten, hingga pencurian data.

Atas dasar itu, Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT) menyusun panduan ini sebagai acuan praktis bagi seluruh pegawai dalam mengelola kata sandi dan autentikasi. Panduan disajikan ringkas dan langsung dapat diterapkan tanpa memerlukan latar belakang teknis yang mendalam.

Kepada semua pihak yang telah memberikan masukan dalam penyusunan panduan ini, kami sampaikan penghargaan dan terima kasih. Saran perbaikan untuk edisi berikutnya dapat disampaikan melalui kanal resmi KUTIM-CSIRT.

Sangatta, Mei 2026

Tim Tanggap Insiden Siber
Kabupaten Kutai Timur

KUTIM-CSIRT

Daftar Isi

BAB 1

Pendahuluan

1.1 Latar Belakang

Akun pengguna dan kata sandi adalah kunci utama yang melindungi sistem informasi, surel resmi, basis data, dan layanan daring di lingkungan pemerintah daerah. Pengamanan sistem yang paling canggih sekalipun menjadi tidak berarti apabila kata sandi yang melindunginya dapat ditebak atau jatuh ke tangan yang salah.

Penanganan insiden yang dilakukan KUTIM-CSIRT menunjukkan bahwa penyalahgunaan akun dengan kata sandi lemah merupakan jalan masuk paling umum bagi gangguan keamanan siber. Akun yang memakai kata sandi sederhana, digunakan ulang di banyak layanan, atau tidak pernah diganti memberi peluang besar bagi pihak tidak berwenang untuk mengambil alih. Setelah satu akun dikuasai, gangguan dapat menyebar ke layanan lain yang memakai kata sandi yang sama.

Sebagian besar risiko tersebut dapat dihilangkan melalui kebiasaan pengelolaan kata sandi yang baik dan penerapan autentikasi tambahan. Langkah-langkah ini sederhana, tidak memerlukan biaya khusus, dan dapat segera dilakukan oleh setiap pegawai.

1.2 Maksud dan Tujuan

Panduan ini disusun dengan maksud menyediakan acuan tunggal yang ringkas bagi pegawai dalam mengelola kata sandi dan autentikasi akun secara aman. Tujuannya adalah:

- menyamakan pemahaman tentang ancaman yang membidik akun dan kata sandi;
- memberikan cara menyusun kata sandi yang kuat dan mudah dijaga;
- memperkenalkan autentikasi dua faktor sebagai lapisan perlindungan tambahan;
- menyediakan daftar periksa untuk menilai kebiasaan keamanan akun secara mandiri;
- menjelaskan langkah yang harus diambil apabila akun diduga disusupi.

1.3 Ruang Lingkup

Panduan ini mencakup pengelolaan kata sandi dan autentikasi untuk seluruh akun yang digunakan dalam pelaksanaan tugas, baik akun surel, sistem aplikasi internal, layanan pemerintahan berbasis elektronik, maupun akun pendukung lainnya. Panduan ini tidak membahas pengamanan teknis tingkat lanjut pada infrastruktur, yang penanganannya dikoordinasikan langsung dengan KUTIM-CSIRT.

1.4 Sasaran Pengguna

Dokumen ini ditujukan bagi seluruh pegawai dan Aparatur Sipil Negara di lingkungan Pemerintah Kabupaten Kutai Timur, serta pengelola sistem pada setiap Perangkat Daerah. Pimpinan Perangkat Daerah dapat menggunakan panduan ini untuk memastikan kebiasaan pengelolaan akun yang baik telah diterapkan oleh seluruh jajarannya.

1.5 Dasar Acuan

- Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
- Peraturan Badan Siber dan Sandi Negara mengenai penyelenggaraan keamanan siber dan pembentukan Tim Tanggap Insiden Siber pada instansi pemerintah;
- Keputusan Bupati Kutai Timur Nomor 555/K.557/2024 tentang Pembentukan Tim Tanggap Insiden Siber Kabupaten Kutai Timur.

BAB 2

Ancaman terhadap Akun dan Kata Sandi

Pegawai perlu mengenali cara-cara yang umum dipakai untuk menguasai akun agar dapat menempatkan langkah perlindungan secara tepat. Penjelasan berikut bersifat umum dan edukatif; rincian teknis yang dapat disalahgunakan sengaja tidak dicantumkan.

No	Bentuk Ancaman	Uraian Singkat dan Dampak
1	**Penebakan kata sandi lemah**	Percobaan masuk dengan mencoba kata sandi yang umum atau mudah ditebak, seperti tanggal lahir atau pola sederhana. Kata sandi pendek dan tidak unik dapat ditembus dalam waktu sangat singkat.
2	**Pemakaian ulang kata sandi** lintas layanan	Penggunaan kata sandi yang sama pada banyak akun. Apabila satu layanan bocor, seluruh akun lain yang memakai kata sandi itu ikut terbuka tanpa perlu usaha tambahan.
3	**Kebocoran kredensial** dari layanan lain	Kata sandi yang bocor dari layanan pihak ketiga dikumpulkan dan dicoba pada akun pemerintahan. Akun resmi menjadi terancam meskipun sistem instansi sendiri tidak bermasalah.
4	**Pengelabuan** (*phishing*) untuk mencuri kata sandi	Pesan atau halaman palsu yang menyerupai layanan resmi dan memancing pegawai memasukkan kata sandinya. Kata sandi yang diketik langsung diterima oleh pihak yang tidak berwenang.
5	**Kata sandi bawaan** yang tidak diganti	Kata sandi awal dari pengembang atau penyedia jasa yang dibiarkan tetap digunakan. Kata sandi semacam ini umumnya diketahui luas dan menjadi sasaran pertama percobaan masuk.

CATATAN

Ancaman terhadap akun jarang berdiri sendiri. Kata sandi yang bocor dari satu layanan kerap dipakai untuk menguasai akun lain melalui pemakaian ulang, dan akun yang dikuasai dapat dipakai mengirim pesan pengelabuan ke rekan kerja. Karena itu, kebiasaan baik pada Bab 3 dan 4 perlu diterapkan untuk seluruh akun, bukan sebagian.

BAB 3

Menyusun Kata Sandi yang Kuat

Kata sandi yang kuat adalah pertahanan pertama setiap akun. Bab ini menjelaskan cara menyusunnya, hal yang harus dihindari, serta alat bantu yang memudahkan pengelolaannya.

3.1 Prinsip Kata Sandi yang Kuat

Kekuatan kata sandi tidak ditentukan oleh seberapa rumit ia terlihat, melainkan oleh seberapa sulit ia ditebak atau dicoba secara otomatis.

- Utamakan panjang. Kata sandi yang panjang jauh lebih sulit ditembus daripada kata sandi pendek meskipun penuh simbol; gunakan sekurang-kurangnya dua belas karakter.
- Gunakan frasa sandi, yaitu rangkaian beberapa kata yang mudah Anda ingat namun tidak mudah ditebak orang lain.
- Buat kata sandi yang unik untuk setiap layanan, sehingga kebocoran pada satu akun tidak menjalar ke akun lain.
- Ganti kata sandi apabila ada dugaan kebocoran, dan tidak perlu menggantinya terlalu sering tanpa alasan karena justru mendorong pemilihan kata sandi yang lemah.

3.2 Hal yang Harus Dihindari

Sejumlah kebiasaan membuat kata sandi mudah ditebak dan harus dihindari.

- Data pribadi yang mudah diketahui, seperti nama, tanggal lahir, nomor telepon, atau nama instansi.
- Pola umum yang lazim dicoba, seperti urutan angka, urutan huruf pada papan ketik, atau kata yang ditambah angka di belakangnya.
- Pemakaian ulang kata sandi pada beberapa akun sekaligus, termasuk antara akun pribadi dan akun kedinasan.
- Menuliskan kata sandi pada catatan yang mudah terlihat atau menyimpannya dalam berkas tanpa pelindung.
- Membagikan kata sandi kepada orang lain, termasuk rekan kerja, melalui pesan atau lisan.

3.3 Aplikasi Pengelola Kata Sandi

Menjaga kata sandi yang panjang dan berbeda untuk setiap layanan sulit dilakukan dari ingatan. Aplikasi pengelola kata sandi (*password manager*) membantu menyimpan seluruh kata sandi secara terenkripsi dan memanggilnya saat dibutuhkan.

- Pengguna cukup mengingat satu kata sandi induk yang kuat untuk membuka aplikasi; kata sandi lain disimpan dan dimasukkan oleh aplikasi.
- Aplikasi dapat membuatkan kata sandi acak yang panjang dan unik untuk setiap akun baru.
- Pilih aplikasi yang bereputasi baik, lindungi kata sandi induknya dengan autentikasi dua faktor, dan jangan menyimpan kata sandi induk di tempat yang tidak aman.

> **CATATAN**
>
> Peramban web juga dapat menyimpan kata sandi. Fitur ini boleh dipakai untuk akun yang risikonya rendah, namun untuk akun kedinasan yang penting sebaiknya gunakan aplikasi pengelola kata sandi tersendiri dan pastikan perangkat selalu terkunci saat ditinggalkan.

BAB 4

Autentikasi Dua Faktor dan Pengelolaan Akun

Kata sandi yang kuat perlu didukung lapisan kedua. Bab ini menjelaskan autentikasi dua faktor serta tata kelola akun yang baik di lingkungan kerja.

4.1 Mengenal Autentikasi Dua Faktor

Autentikasi dua faktor (2FA) menambahkan satu langkah verifikasi setelah kata sandi dimasukkan. Selain mengetahui kata sandi, pengguna juga harus membuktikan kepemilikan atas sesuatu, biasanya berupa kode sementara atau perangkat tertentu. Dengan demikian, kata sandi yang bocor saja tidak cukup bagi pihak lain untuk masuk ke akun. Autentikasi dua faktor sangat dianjurkan untuk seluruh akun penting, terutama surel dan sistem aplikasi pemerintahan.

4.2 Jenis Autentikasi Dua Faktor

- **Aplikasi autentikator.** Aplikasi pada telepon genggam yang menghasilkan kode sementara secara berkala. Tidak memerlukan jaringan dan lebih aman daripada kode melalui SMS.
- **Kode melalui SMS.** Kode dikirim sebagai pesan singkat ke nomor telepon terdaftar. Mudah digunakan, namun lebih rentan disadap dan bergantung pada sinyal; dipakai bila pilihan lain tidak tersedia.
- **Kunci keamanan fisik.** Perangkat kecil yang dihubungkan ke komputer atau telepon untuk memverifikasi masuk. Memberi perlindungan paling kuat, termasuk terhadap pengelabuan, dan disarankan untuk akun yang sangat penting.

4.3 Cara Mengaktifkan

Sebagian besar layanan menyediakan pengaturan ini pada menu keamanan akun. Secara umum, langkahnya:

1. Buka menu pengaturan keamanan akun dan pilih opsi autentikasi dua faktor atau verifikasi dua langkah.
2. Pilih jenis yang akan digunakan, lalu ikuti petunjuk untuk menautkan aplikasi autentikator, nomor telepon, atau kunci keamanan.
3. Simpan kode pemulihan yang diberikan di tempat yang aman; kode ini dipakai apabila perangkat utama hilang.
4. Lakukan satu kali percobaan masuk untuk memastikan autentikasi dua faktor telah berfungsi.

4.4 Pengelolaan Akun di Lingkungan Kerja

Selain kata sandi dan autentikasi, tata kelola akun di setiap Perangkat Daerah turut menentukan keamanan secara keseluruhan.

- Hindari akun bersama yang dipakai banyak orang; setiap pegawai sebaiknya memakai akun atas namanya sendiri agar aktivitas dapat ditelusuri.
- Nonaktifkan akun pegawai yang pindah tugas, purnatugas, atau penyedia jasa yang masa kerjanya berakhir.
- Berikan hak akses seminimal yang diperlukan untuk tugas masing-masing; peran administrator hanya untuk yang benar-benar membutuhkannya.
- Tinjau daftar akun dan hak aksesnya secara berkala, sekurang-kurangnya setiap tiga bulan.

BAB 5

Daftar Periksa dan Penanganan Akun Bermasalah

5.1 Daftar Periksa Tata Kelola Kata Sandi

Daftar periksa berikut digunakan untuk menilai kebiasaan keamanan akun secara mandiri. Beri tanda pada kolom status untuk setiap butir yang telah dipenuhi, dan jadikan butir yang belum terpenuhi sebagai prioritas perbaikan.

No	Butir Tata Kelola	Sudah
A. KATA SANDI		
1	Setiap akun memakai kata sandi yang panjang, minimal dua belas karakter.	☐
2	Tidak ada kata sandi yang dipakai ulang pada lebih dari satu akun.	☐
3	Kata sandi tidak memuat data pribadi atau pola umum.	☐
4	Seluruh kata sandi bawaan telah diganti.	☐
5	Kata sandi disimpan dengan aman, tidak pada catatan terbuka.	☐
B. AUTENTIKASI		
6	Autentikasi dua faktor diaktifkan pada akun surel dan sistem penting.	☐
7	Kode pemulihan autentikasi dua faktor disimpan di tempat aman.	☐
8	Aplikasi pengelola kata sandi dilindungi kata sandi induk yang kuat.	☐
C. PENGELOLAAN AKUN		
9	Tidak ada akun bersama untuk tugas yang seharusnya per pengguna.	☐
10	Akun pegawai yang pindah atau purnatugas telah dinonaktifkan.	☐
11	Hak akses diberikan seminimal yang diperlukan.	☐
12	Daftar akun dan hak akses ditinjau berkala, minimal tiga bulan sekali.	☐

5.2 Tanda Akun Diduga Disusupi

Pegawai perlu waspada terhadap tanda-tanda berikut:

- pemberitahuan masuk dari perangkat atau lokasi yang tidak dikenali;
- kata sandi tiba-tiba tidak berlaku padahal tidak pernah diganti;
- terkirimnya pesan atau surel dari akun tanpa sepengetahuan pemiliknya;
- perubahan pengaturan akun, seperti nomor pemulihan, yang tidak dilakukan sendiri;
- munculnya aktivitas yang tidak dikenali pada riwayat akun.

5.3 Langkah Penanganan dan Pelaporan

Apabila akun diduga disusupi, lakukan langkah berikut dengan segera.

1. Ganti kata sandi akun dari perangkat lain yang terpercaya dan bebas dari program berbahaya.
2. Keluar dari seluruh sesi yang aktif melalui menu keamanan akun agar akses pihak lain terputus.
3. Periksa riwayat dan pengaturan akun, lalu kembalikan perubahan yang tidak dikenali.
4. Aktifkan autentikasi dua faktor bila belum terpasang.
5. Laporkan kejadian kepada KUTIM-CSIRT, terutama bila akun terkait layanan kedinasan.

> **PENTING**
>
> Bila akun yang sama dipakai pada beberapa layanan, ganti pula kata sandi pada layanan lain tersebut. Jangan mengganti kata sandi dari perangkat yang diduga bermasalah, karena kata sandi baru dapat ikut terbaca oleh pihak yang tidak berwenang.

Saat melapor, sertakan informasi sejelas mungkin: nama akun atau layanan yang terdampak, waktu dan gejala yang ditemukan, serta langkah yang sudah dilakukan. Pelaporan dapat disampaikan melalui kanal berikut.

Kanal Pelaporan Insiden — KUTIM-CSIRT

Formulir daring	**csirt.kutaitimurkab.go.id/lapor**
Surel	**csirt@kutaitimurkab.go.id**
Telepon	**(0549) 2021207 — pada jam kerja**
Lacak laporan	**csirt.kutaitimurkab.go.id/lacak-tiket**

PENUTUP

Penutup

Mengelola kata sandi dan autentikasi dengan baik bukanlah pekerjaan sekali selesai, melainkan kebiasaan yang dijaga setiap hari oleh setiap pegawai. Langkah-langkah dalam panduan ini sederhana dan tidak memerlukan biaya khusus, namun memberikan perlindungan yang nyata terhadap sebagian besar gangguan keamanan yang membidik akun.

KUTIM-CSIRT terbuka untuk membantu Perangkat Daerah dalam menerapkan panduan ini, baik melalui sosialisasi, peninjauan kesiapan keamanan akun, maupun penanganan insiden. Panduan ini akan ditinjau secara berkala dan diperbarui sesuai perkembangan ancaman serta masukan dari para pengguna.

PERNYATAAN DOKUMEN

Dokumen ini diterbitkan oleh Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT) di bawah Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Kutai Timur. Dokumen berklasifikasi TERBUKA dan boleh disebarluaskan di lingkungan pemerintah maupun masyarakat untuk tujuan peningkatan keamanan siber.

— SELESAI —