<table>
<tr><td rowspan="6">KEMENTRIAN PENDIDIKAN,
KEBUDAYAAN, RISET
DAN TEKNOLOGI
UNIVERSITAS NUSA CENDANA
UPT. TIK
email : info@undana.ac.id, website :
https://tik.undana.ac.id</td><td>Nomor Pos</td><td>:</td><td></td></tr>
<tr><td>Tanggal Pembuatan</td><td>:</td><td>16 Maret 2023</td></tr>
<tr><td>Tanggal revisi</td><td>:</td><td></td></tr>
<tr><td>Tanggal Evektif</td><td>:</td><td></td></tr>
<tr><td>Disahkan oleh</td><td>:</td><td>Kepala UPT. TIK

Dr. Kalvein Rantelobo, ST.,MT
NIP. 19710617 199903 1 003</td></tr>
<tr><td>Nama Pos</td><td>:</td><td>Penggunaan Akses Kontrol</td></tr>
<tr><td colspan="3">Dasar Hukum</td><td>Kualifikasi Pelaksana</td></tr>
<tr><td colspan="3">1. Undang-undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional
2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor : 35 Tahun 2012 tentang Penyusunan Standart Operasional Prosedur
3. Keputusan Menteri Pendidikan , Kebudayaan, Riset dan Teknologi Nomor: 25 Tahun 2021 Tentang Organisasi dan Tata Kerja Universitas Nusa Cendana
4. Keputusan Rektor Undana Nomor 3 Tahun 2019 tentang Pedoman Penyelenggaraan Pendidikan di Universitas Nusa Cendana
5. Peraturan Pemerintah No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik
6. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor : 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.</td><td>1. S1
2. Mengetahui tugas dan fungsi
3. Mengetahui POS Penggunaan Akses Kontrol</td></tr>
<tr><td colspan="3">Keterkaitan</td><td>Peralatan dan Kelengkapan</td></tr>
<tr><td colspan="3">1. Pos masuk ruang server</td><td>1. Pakta integritas</td></tr>
<tr><td colspan="3">Peringatan</td><td>Pencatatan dan Pendataan</td></tr>
<tr><td colspan="3"></td><td>1. Invetraris asset
2. Inventaris perangkat bergerak</td></tr>
</table>

1. TUJUAN :

Untuk memastikan bahwa kebijakan register dan unregister dari User untuk mengakses system & Jaringan yang disediakan oleh UPT. TIK dalam keadaan aman dan tepat termasuk persyaratan dalam memberikan akses *user* secara istimewa kepada pihak yang membutuhkan serta perubahan dalam pola pekerjaan dari *user*.

2. LINGKUP :

Prosedur ini dijalankan untuk semua *user account* yang disediakan UPT. TIK bagi semua staf baik PNS maupun kontrak serta pihak lain yang diberi akses oleh UPT. TIK.

3. TANGGUNGJAWAB :

Kepala UPT. TIK akan memberlakukan Kebijakan ini sebagai penanggungjawab dari Pemilik Proses adalah :

- Memastikan bahwa dokumen yang digunakan saat ini adalah paling terbaru/ *up to date* sesuai dengan persyaratan yang berlaku dan terbaik saat ini.
- Melakukan peninjauan atas proses yang berjalan untuk memastikan keseusaian dan kepatuhan yang berlaku saat ini.

4. DOCUMENT CONTROL :

Untuk memastikan bahwa user menggunakan dokumen yang terbaru/ *up to date* dan semua form referensi yang tersedia di WJ-IMS (Intranet).

5. PENCATATAN DOKUMEN :

IMS-SOP-No.2 Pengendali Dokumen untuk mengidentifikasi persyaratan penyimpanan dokumen untuk semua dokumen yang digunakan dalam prosedur ini.

6. CONTINUOUS IMPROVEMENT :

Perbaikan atas Bisnis Proses dapat dilakukan kepada user untuk evaluasi.

7. ISO ELEMENTS :

ISO27001: 2013

KEBIJAKAN AKSES KONTROL

PENANGGUNG JAWAB

Semua divisi dengan koordinasi kepala UPT. TIK bertanggungjawab memberikan informasi segera kepada civitas akademika kebijakan akses control dikarenakan :

- Staf baru membutuhkan akses untuk jaringan dan system
- Staf yang sudah mengundurkan diri atau yang tidak membutuhkan untuk mengakses jaringan dan sistem
- Staf yang membutuhkan akses untuk jaringan yang berbeda atas dasar perubahan pekerjaan.

  Kepala UPT. TIK agar selalu melakukan pengecekan atas akses control jaringan dan system untuk memastikan bahwa *user* yang sudah non aktif sudah dinon aktifkan dan *user* yang ada sesuai dengan fungsi dan hak akses nya.

HAK AKSES YANG UNIK SERTA AKSES KONTROL UNTUK PERLU DIKETAHUI

Hak akses masing-masing pengguna harus disesuaikan dengan kebutuhan dari masing-masing *user*. Hak *user* untuk semua akses harus berdasarkan fungsi dan klasifikasi pekerjaannya. Koordinator divisi harus mempunyai akses untuk men'default;" menghapus semua akses. Ini termasuk proses pengembangan system untuk sumber data dan testing data.

Setiap *user* harus menggunakan ID yang unik dan password pribadi untuk mengakses jaringan dan sistem. Dilarang menggunakan *user* pengguna yang tidak diautentikasi (misalnya tanpa kata sandi) atau *user* yang tidak terkait dengan satu pengguna yang teridentifikasi.

User bersama atau grup tidak diizinkan untuk akses system. Namun, kemungkinan teknologi yang digunakan tidak selalu memfasilitasi kebutuhan ini. Dalam kasus seperti itu, divisi Sistem Informasi harus memastikan bahwa kontrol kompensasi untuk mengaudit dan memantau kegiatan individu. Pengecualian kebijakan tersebut harus disetujui oleh Kepala UPT. TIK dan dicatat.

Dalam 28 hari setelah diizinkan mengakses jaringan dan sistem, semua *user* harus memahami tentang kebijakan keamanan informasi dengan membaca dan menandatangani pakta integritas tentang :

- Kebijakan Keamanan Informasi
- Kebijakan Penggunaan yang Dapat Diterima

Jika tidak, akses ke jaringan dan sistem akan ditangguhkan.

Apabila akses telah diberikan ke jaringan dan sistem sebelum versi kebijakan ini diterbitkan, kebijakan akan berlaku secara retrospektif.

User yg terdaftar ke program pelatihan Kesadaran Keamanan Informasi organisasi – kegagalan untuk menyelesaikan materi kursus dapat mengakibatkan penangguhan atau pembatasan akses ke jaringan dan system.

USER BARU

Langkah-langkah berikut harus diambil untuk mendaftarkan *user* baru untuk mengakses jaringan dan sistem.

TANGGUNG JAWAB SETIAP DIVISI

Setiap Divisi harus memastikan bahwa :

1. Semua *user* baru telah menerima pelatihan pengenalan tentang penggunaan jaringan dan sistem. Ini harus mencakup tinjauan umum kebijakan keamanan informasi, termasuk kebijakan keamanan informasi dan penggunaan yang dapat dipertanggungjawabkan.
2. Komunikasi formal (menggunakan SOP yang disetujui) dikirim ke ujit-unit untuk meminta agar pengguna diberikan akses ke jaringan dan sistem dan aplikasi yang dipilih, termasuk tingkat akses yang diperlukan.
3. Informasi yang harus disediakan adalah :
    a. Nama Lengkap *User*
    b. Deskripsi peran dan area jaringan dan sistem IT yang harus diakses oleh *user* untuk menjalankan peran mereka.
    c. Apakah *user* adalah pegawai tetap, pegawai tidak tetap, kontraktor atau pihak ketiga. Untuk semua posisi selain pegawai tetap, tanggal terakhir bekerja juga diperlukan.

TANGGUNG JAWAB DEPARTEMEN IT

Kepala UPT. TIK memastikan bahwa :

1. Sebuah akun domain jaringan yang unik dialokasikan untuk setiap pengguna baru
2. Hak akses yang diminta diberikan, dan ini sejalan dengan prinsip perlu-tahu, yaitu setiap *user* baru tidak akan diberikan hak istimewa selain yang diperlukan untuk melakukan peran pekerjaan mereka.
3. Komunikasi formal (menggunakan SOP yang disetujui) dikirim ke unit-unit yang meminta akun *user* dan kewenangan yang baru, untuk mengonfirmasi bahwa akun *user* dan hak akses telah diatur sesuai permintaan.
4. *Log in up-to-date* dari semua permintaan akses, dan akun *user* dan kewenangan yang diberikan dipertahankan;
5. Pengguna sementara dihapus segera setelah periode akses yang diperlukan telah habis.

USER MENGUNDURKAN DIRI/ RESIGN

Langkah-langkah berikut harus diambil untuk mendaftarkan *user* baru untuk mengakses jaringan dan sistem.

TANGGUNG JAWAB SETIAP MANAJER

Setiap divisi harus memastikan bahwa :

1. Ketika staf IT mengundurkan diri, atau diberhentikan, coordinator divisi harus, berkonsultasi dengan kepala UPT. TIK, menilai apakah akses pengguna ke jaringan dan sistem selama periode pemberitahuan menimbulkan risiko keamanan;
2. Jika akses user menimbulkan risiko, akses ke jaringan dan sistem harus segera ditarik;
3. Jika user tidak menimbulkan risiko keamanan, akses ke IT akan dinonaktifkan pada hari terakhir kerja.
4. Komunikasi formal (Pengguna user dari IT yang disetujui) dikirim unit-unit untuk meminta *user* akses ke jaringan dan sistem untuk dinonaktifkan;
5. Informasi yang harus disediakan adalah :
    i. Nama Lengkap *User*
    ii. Tanggal penonaktifan *user*
    iii. Daftar semua akun dari *user* yang harus dicabut.
6. Komunikasi formal (menggunakan standar yang disetujui) dikirim ke manajer HRD untuk memberi tahu mereka bahwa karyawan akan meninggalkan kantor dan memberikan tanggal resign dan perincian bangunan, kantor, kamar, dan fasilitas yang dimiliki oleh karyawan serta akses kode atau tombol akses ke semua nya.
7. Pada hari terakhir kerja, kepala UPT. TIK harus memastikan bahwa semua properti dari asset yang diberikan kepada staf tersebut dikembalikan (misalnya laptop, Personal Digital Assistant (PDA), telepon seluler, perangkat akses fisik).
8. Jika peran *user* berubah atau pengguna berpindah ke peran baru dan akses tidak lagi diperlukan untuk sistem tertentu, maka kepala UPT. TIK bertanggung jawab untuk memastikan izin akses pengguna diubah sesuai dengan itu.

TANGGUNG JAWAB UPT. TIK

Kepala UPT. TIK memastikan bahwa :

1. Semua *user* pengguna *system* yang relevan akan dihapus/dinonaktifkan, termasuk semua hak akses.
2. Komunikasi formal (menggunakan SOP yang disetujui) dikirim ke unit yang mengajukan permintaan penghapusan untuk mengonfirmasi bahwa *user* telah dihapus/dinonaktifkan, termasuk semua hak akses.

3. *Log in up-to-date* dipertahankan dari semua permintaan unregistrasi, dari hak istimewa yang dicabut.

USER MUTASI/ PINDAH UNIT LAIN

Ketika peran staf berubah di dalam fungsi dan tugasnya, hak akses (dan fisik) harus diubah sebagaimana mestinya.

Langkah-langkah berikut harus diambil untuk mendaftarkan user baru untuk mengakses jaringan dan sistem.

TANGGUNG JAWAB SETIAP UNIT

Setiap unit harus memastikan bahwa :

1. Komunikasi formal (menggunakan SOP yang disetujui) dikirim ke UPT. TIK untuk meminta hak akses pengguna diubah;
2. Informasi yang harus disediakan adalah :
   i. Nama Lengkap *User*
   ii. Deskripsi peran baru *user* dan area jaringan dan sistem yang memerlukan akses *user* untuk melakukan peran barunya
   iii. Bila perlu, area jaringan dan sistem yang tidak lagi diperlukan akses *user*
   iv. Entah itu perubahan permanen atau sementara. Untuk perubahan sementara, berikan tanggal terakhir akses akan diperlukan.

TANGGUNG JAWAB UPT. TIK

UPT. TIK memastikan bahwa :

1. Semua *user* pengguna *system* yang relevan akan dihapus/dinonaktifkan, termasuk semua hak akses
2. Komunikasi formal (menggunakan SOP yang disetujui) dikirim ke pimpinan unit yang mengajukan permintaan penghapusan untuk mengonfirmasi bahwa *user* telah dihapus/dinonaktifkan, termasuk semua hak akses.
3. *Log in up-to-date* dipertahankan dari semua permintaan unregistrasi, dari hak istimewa yang dicabut.
4. Hak akses sementara akan dihapus setelah periode akses yang diperlukan telah berakhir (misalnya dengan menggunakan *Microsoft Active Directory*).

TINJAUAN REGULER HAK & WEWENANG AKSES USER

Kepala UPT. TIK harus memastikan bahwa tinjauan berkala atas hak akses dan wewenang dilakukan. Ini akan berlaku untuk semua jenis jaringan, sistem operasi, aplikasi, dan akun pengguna basis data untuk memastikan bahwa akun yang tidak dipakai telah dihapus atau dinonaktifkan, yang ada sudah sesuai.

Setiap divisi melakukan pemeriksaan setiap tiga bulan untuk memverifikasi bahwa hak akses pengguna dikelola dengan benar, wewenang yang tidak perlu akan dihapus. Hak akses khusus (termasuk akses 'administrator TI') juga harus ditinjau setiap triwulan; ulasan ini juga harus mencakup berikut ini:

- Konfirmasi bahwa pemisahan tugas yang memadai telah diterapkan, terutama untuk peran staf dengan hak akses wewenng akses lebih luas.
- Penonaktifan akun milik staf yang sudah ada setelah 60 hari tidak aktif

SYARAT PEMBUATAN PASSWORD

Kebijakan tentang penggunaan password yang aman didokumentasikan serta Kebijakan Penggunaan Keamanan Informasi yang Dapat Diterima . Kebijakan ini berlaku untuk kata sandi yang digunakan untuk semua jenis akun pengguna jaringan, sistem operasi, aplikasi dan basis data yang berbeda.

Selain itu, kebijakan berikut berlaku :

1. *Password* pertama kali diberikan oleh UPT. TIK untuk *user* baru dan pengaturan ulang kata sandi harus unik, yaitu setiap kata sandi dibuat secara acak;
2. UPT. TIK akan memverifikasi identitas pengguna yang memerlukan *reset password*, sebelum melakukan *reset password*, mis. menggunakan metode standar IT yang disetujui yang melibatkan komunikasi formal dengan kepala UPT. TIK.