<table>
<tr><td rowspan="6">KEMENTRIAN PENDIDIKAN,
KEBUDAYAAN, RISET
DAN TEKNOLOGI
UNIVERSITAS NUSA CENDANA
UPT. TIK
email : puskom@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 JARAK JAUH</td></tr>
<tr><td colspan="2">Dasar Hukum</td><td colspan="2">Kualifikasi Pelaksana</td></tr>
<tr><td colspan="2">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 colspan="2">1. S1
2. Mengetahui tugas dan fungsi
3. Mengetahui POS Penggunaan Akses Jarak Jauh</td></tr>
<tr><td colspan="2">Keterkaitan</td><td colspan="2">Peralatan dan Kelengkapan</td></tr>
<tr><td colspan="2">1. Pos masuk ruang server</td><td colspan="2">1. Pakta integritas</td></tr>
<tr><td colspan="2">Peringatan</td><td colspan="2">Pencatatan dan Pendataan</td></tr>
<tr><td colspan="2"></td><td colspan="2">1. Invetraris asset
2. Inventaris perangkat bergerak</td></tr>
</table>

1. TUJUAN :

Kebijakan ini memastikan bahwa Undana menerapkan praktik terbaik keamanan informasi untuk para staf yang mengakses Jarak Jauh untuk mempertahankan kepatuhan berkelanjutan terhadap ISO 27001.

Kebijakan ini menegaskan tanggung jawab para staf yang mengakses Jarak Jauh untuk keamanan penggunaan semua peralatan yang ada di rumah; mengamankan akses jarak jauh dari infrastruktur jaringan, sehingga meminimalkan ancaman pengungkapan informasi yang tidak sah, atau kehilangan informasi dan peralatan.

2. LINGKUP :

Kebijakan ini berlaku untuk semua orang yang menyelesaikan pekerjaan yang berada di lapangan dan pekerjaan di rumah sebagai kelanjutan dari pekerjaan mereka dengan Undana.

3. TANGGUNGJAWAB :

Bagi staf/ Pihak Ketiga harus selalu bekerja sesuai dengan Kebijakan dan prosedur yang ditetapkan oleh UPT. TIK.

Kepala UPT. TIK bertanggung jawab untuk mengizinkan staf yang mengakses kerja jarak jauh dalam tim mereka.

Divisi Teknologi Jaringan bertanggung jawab untuk menerapkan kontrol untuk akses jarak jauh yang aman ke jaringan dan untuk peralatan yang aman.

Pemilik Proses bertanggung jawab untuk:

- Meninjau isi/ konten secara berkala untuk memastikan dokumen terkini dan terbaru dengan persyaratan hukum dan praktik terbaik saat ini.
- Melakukan tinjauan konten tahunan secara formal untuk memastikan kepatuhan dan kesesuaian.

Setiap pelanggaran terhadap kebijakan ini dapat mengakibatkan tindakan disipliner staf, atau tuntutan hukum dan/atau pelanggaran kontrak.

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

DEFINISI AKSES JARAK JAUH

Mengakses pekerjaan secara Jarak Jauh adalah pekerja dari staf yang telah diberi wewenang untuk menggunakan fasilitas pemrosesan informasi dan informasi IT sementara yang tidak berada di lokasi Undana. Mengakses pekerjaan secara jarak jauh harus selalu mematuhi kebijakan ini.

Perlengkapan peralatan IT apa saja yang digunakan tidak terbatas pada laptop, tablet dan telepon genggam.

KEBIJAKAN MENGAKSES PEKERJAAN SECARA JARAK JAUH

Kebijakan mengakses pekerjaan secara jarak jauh harus diberi wewenang oleh Kepala UPT. TIK.

Persyaratan Keamanan Fisik:

Langkah-langkah berikut diperlukan untuk mengurangi risiko ancaman keamanan fisik terhadap Peralatan dan informasi yang mengakses pekerjaan secara Jarak Jauh :

1. Peralatan tidak boleh ditinggalkan tanpa pengawasan yang tidak terlindungi
2. Jika memungkinkan, Peralatan harus disimpan di dalam lemari, meja, atau ruangan yang terkunci saat tidak digunakan, dan kunci terkait harus dilindungi untuk mencegah akses tidak sah ke Peralatan
3. Jika fasilitas yang terkunci tidak tersedia, laptop harus diamankan menggunakan perangkat pencegah pencurian seperti kabel yang dapat dikunci, mis. kunci Kensington.
4. Saat berada di dalam kantor, Peralatan yang tidak aman tidak boleh dibiarkan tanpa pengawasan untuk waktu yang lama di area terbuka atau kantor yang tidak terkunci, dan pada malam hari, perangkat seluler harus diamankan secara fisik atau dikunci agar tidak terlihat.
5. Token akses keamanan elektronik apa pun yang dikeluarkan harus disimpan terpisah dari laptop atau PC mana pun saat dibiarkan tanpa pengawasan, jika tidak, akses tidak sah ke jaringan dan sistem di IT dapat terjadi.
6. Peralatan komputer tidak boleh ditinggalkan sehingga dapat dengan mudah dilihat melalui jendela lantai dasar oleh orang lain, saat bekerja di rumah.
7. Layar komputer dan printer harus ditempatkan sedemikian rupa sehingga informasi tidak dapat dilihat oleh semua orang , orang yg bekerja di sekitar, keluarga, pengunjung, atau orang lain yang tidak berwenang. Pelindung layar dapat diminta ke IT berdasarkan permintaan.
8. Area kerja yang tenang dan terpisah harus dipilih untuk meminimalisasi dan mengontrol gangguan yang tidak terduga dan kemungkinan informasi sensitif dilihat oleh orang yang tidak berwenang.
9. Anggota keluarga, teman, pengunjung, atau siapa pun tidak boleh menggunakan peralatan yang diberikan UPT. TIK.

10. Kebijakan clear desk harus diterapkan untuk semua dokumentasi fisik , file, dan media komputer yang dapat dipindahkan, mis. Stik memori USB harus disimpan dengan aman saat ditinggalkan, dan media yang dapat dilepas harus dikeluarkan dari komputer saat tidak digunakan.
11. Kebijakan layar terkunci harus diikuti dan bila dibiarkan tanpa pengawasan, peralatan harus log-off atau diamankan dengan screen saver yang dilindungi kata sandi.
12. Saat membawa peralatan dengan kendaraan, perangkat dapat dikunci agar tidak terlihat oleh lain, dan tidak boleh ditinggalkan di kendaraan untuk waktu yang lama atau semalaman.
13. Laptop/ computer harus dibawa dengan tas saat bepergian dengan pesawat.
14. Perangkat laptop/ computer tidak boleh dibiarkan tanpa pengawasan dalam waktu lama di kamar hotel, sehingga memungkinkan akses oleh petugas kebersihan dan orang lain yang tidak berwenang

Persyaratan Keamanan Sistem dan Jaringan Informasi Elektronik

Langkah-langkah berikut diperlukan untuk mengurangi risiko ancaman keamanan terhadap sistem informasi elektronik yaitu informasi dan perangkat lunak dari jaringan perusahaan pada perangkat komputer bergerak dan bekerja di rumah serta pada jaringan dan sistem Undana.

1. Hanya peralatan yang dikeluarkan Undana yang boleh digunakan untuk menghubungkan dengan akses jarak jauh ke jaringan dan sistem Undana.
2. Staf yang bekerja Jarak Jauh hanya boleh mencoba mengakses jaringan dan sistem Undana dengan cara yang telah diizinkan oleh UPT. TIK.
3. Pedoman keamanan password dari IT harus diterapkan. Ini berarti bahwa staf tidak boleh memberikan kata sandi mereka kepada orang lain, dan tidak boleh menuliskan kata sandi.
4. Staf yang bekerja jarak Jauh tidak boleh mengutak-atik atau mengkonfigurasi ulang kontrol dan pengaturan keamanan yang telah diterapkan oleh IT termasuk kontrol untuk akses ke jaringan dan sistem Undana, dan perangkat lunak anti-virus.
5. Staf yang bekerja jarak Jauh harus mematuhi kebijakan Penggunaan Internet dan Email dari luar jaringan Undana.
6. Staf yang bekerja jarak Jauh tidak boleh mengunduh perangkat lunak apa pun ke perangkat komputer bergerak di rumah tanpa izin dari UPT. TIK. Penggunaan perangkat lunak yang tidak sah dapat menyebabkan pelanggaran undang-undang hak cipta atau akses tidak sah ke informasi IT.
7. Perubahan, penambahan, atau peningkatan perangkat keras tidak boleh dilakukan tanpa persetujuan dan keterlibatan UPT.TIK.
8. Staf harus bertanggung jawab & memastikan bahwa file, dokumen, dan 'pekerjaan dalam proses' pada perangkat komputer bergerak dan bekerja di rumah dibackup secara teratur

untuk menghindari kehilangan informasi/ corrupt. Informasi harus disalin secara teratur ke server file Undana yang dbackup secara teratur.

9. Staf harus segera melaporkan setiap insiden keamanan yang nyata atau yang diduga melibatkan perangkat komputer bergerak dan bekerja di rumah kepada divisi SI dan atau divisi system security dan kepala UPT. TIK, termasuk kehilangan, kerusakan atau pencurian peralatan, dan akses tidak sah ke informasi atau jaringan dan sistem Undana.
10. Jika perangkat komputer laptop di rumah dicuri, staf harus segera melaporkan kejadian tersebut ke Polisi.
11. Perlu dicatat bahwa bekerja secara jarak jauh harus dipantau oleh IT, sejalan dengan Kebijakan Keamanan Informasi Undana.

ALAT KONTROL TAMBAHAN

Persyaratan Tambahan untuk Manager Departemen

Manajer Departemen memiliki tanggung jawab tambahan berikut:

1. Kepala UPT. TIK harus secara resmi mengajukan permintaan kepada Undana untuk Peralatan staf yang bekerja Jarak Jauh.
2. Ketika staf tidak lagi membutuhkan Peralatan mis. staf yang berhenti dan berpindah, kepala UPT. TIK harus memastikan bahwa secara resmi sudah diberitahu sesegera mungkin, dan harus memastikan bahwa peralatan yang relevan dikumpulkan dan dikembalikan ke UPT. TIK. Ini harus dicatat secara resmi sebagai bagian dari proses daftar periksa untuk yang meninggalkan atau yang pindah.

Persyaratan Tambahan untuk Departemen IT

Kepala UPT. TIK memiliki tanggung jawab tambahan berikut:

1. Pastikan peralatan dilengkapi dengan label ID aset IT sebelum didistribusikan
2. Harus mengonfigurasi koneksi jarak jauh yang aman dan standar ke jaringan dan sistem Perusahaan untuk semua akses oleh staf yang bekerja jarak jauh.
3. Harus menegakkan implementasi kebijakan password dari Undana.
4. Patch keamanan kritis harus secara otomatis didistribusikan ke semua Peralatan pada kesempatan paling awal.
5. Hanya perangkat lunak standar yang disetujui, sesuai dengan undang-undang hak cipta yang harus diinstal pada semua peralatan IT yang digunakan untuk pekerjaan lapangan dar rumah. IT akan menerapkan kontrol untuk mencegah staf mengonfigurasi ulang atau menambahkan komponen perangkat lunak. Divisi sistem Security menerapkan perlindungan enkripsi pada komputer dan peralatan mobile yang digunakan untuk mobile dan home working.