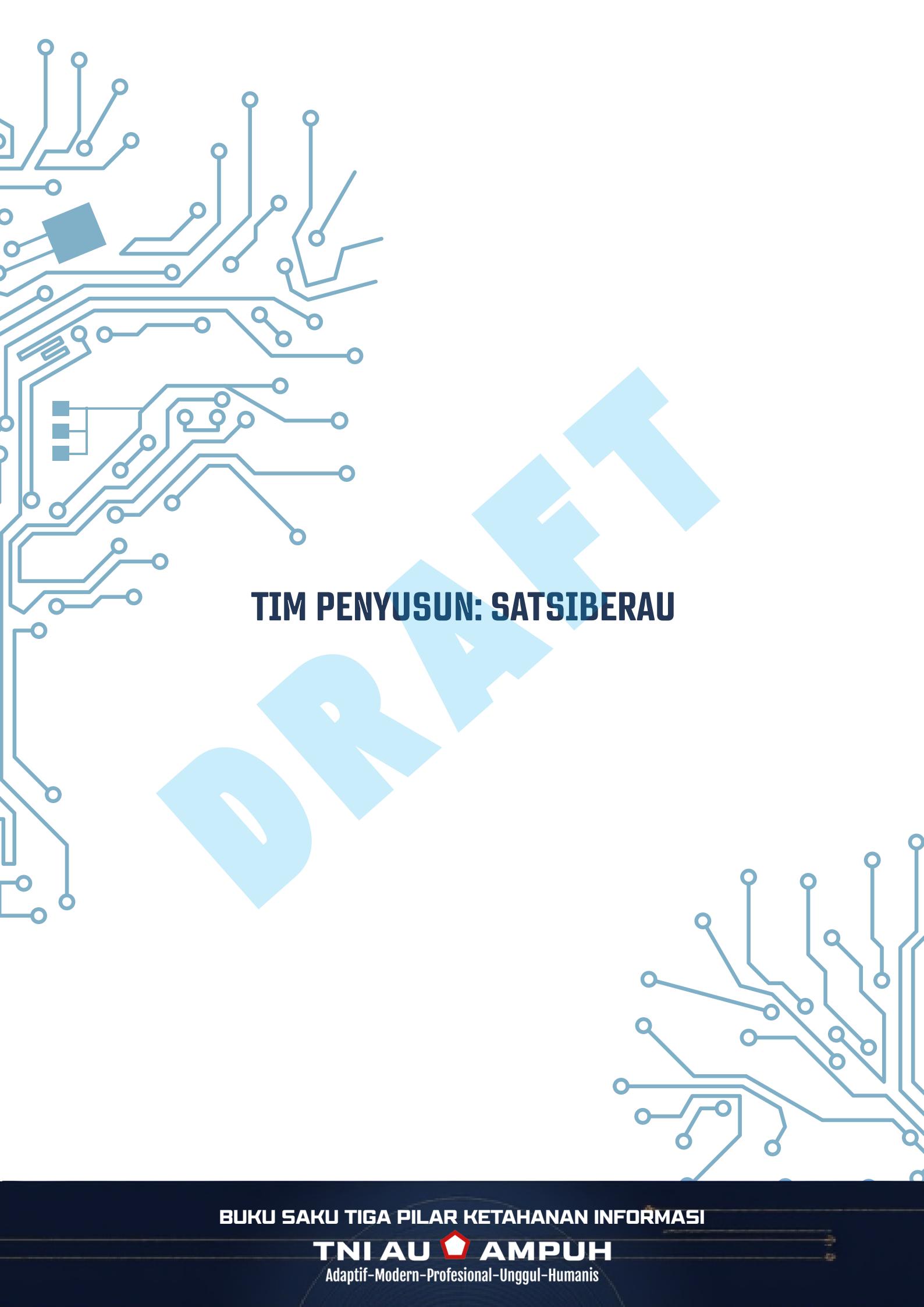




TIGA PILAR KETAHANAN INFORMASI

CYBER SECURITY AWARENESS, KETAHANAN INFORMASI,
DAN ETIKA MEDIA SOSIAL

TNI AU  **AMPUH**
Adaptif-Modern-Profesional-Unggul-Humanis

The background of the slide features a light blue circuit board pattern with various blue lines and nodes, creating a technical and modern aesthetic.

TIM PENYUSUN: SATSIBERAU

DRAFT

BUKU SAKU TIGA PILAR KETAHANAN INFORMASI

TNI AU  **AMPUH**

Adaptif-Modern-Profesional-Unggul-Humanis



KATA PENGANTAR

Perkembangan global menunjukkan bahwa ancaman terhadap kedaulatan negara tidak lagi hanya bersifat konvensional. Perang modern kini juga terjadi di ruang siber dan informasi, senyap namun berdampak besar terhadap opini, moral, dan stabilitas nasional. Karena itu, setiap prajurit TNI AU perlu memahami dan mengantisipasi ancaman non-kinetik, perang kognitif, dan perang informasi.

Perang non-kinetik memanfaatkan teknologi, disinformasi, propaganda, dan serangan siber untuk melemahkan pertahanan tanpa kekuatan fisik. Perang kognitif secara khusus menargetkan cara berpikir, persepsi, emosi, dan pengambilan keputusan individu maupun kelompok guna memengaruhi sikap serta loyalitas terhadap negara. Sementara perang informasi berfokus pada penguasaan narasi dan opini publik melalui ruang digital.

Maka, TNI AU menegaskan pentingnya meningkatkan Cybersecurity Awareness, Ketahanan Informasi, dan Etika Bersosial Media agar seluruh personel mampu bersikap cerdas, waspada, dan bijak dalam menghadapi ancaman modern. Buku saku ini disusun sebagai panduan praktis yang memuat tiga pilar utama: Cybersecurity Awareness, Ketahanan Informasi, dan Etika Bersosial Media. Diharapkan setiap prajurit TNI AU tidak hanya unggul di udara, tetapi juga tangguh di ruang siber dan informasi.

Kepala Staf Angkatan Udara

Marsekal TNI M. Tonny Harjono, S.E., M.M.



DAFTAR ISI

KATA PENGANTAR.....	3
CYBERSECURITY AWARENESS.....	5
KETAHANAN INFORMASI.....	11
ETIKA BERSOSIAL MEDIA.....	17



CYBERSECURITY AWARNESS

1. Keamanan Akun
2. Keamanan Data
3. Peran Pengguna
4. Tanamkan Mindset Zero Trust



TNI AU  **AMPUH**
Adaptif-Modern-Profesional-Unggul-Humanis



CYBERSECURITY AWARENESS

Cybersecurity Awareness adalah pemahaman dan kesadaran seseorang tentang ancaman keamanan digital. Sederhananya, ini risiko saat menggunakan teknologi untuk pribadi dan dinas.

1

CONTOH ANCAMAN

- a. Phishing : Link palsu yang meminta password atau OTP.
- b. Malware : File atau aplikasi berbahaya.
- c. Ransomware : Data dikunci lalu diminta tebusan



2

CARA PENANGANAN

- a. Gunakan password kombinasi huruf besar, kecil, tanda baca, dan angka.
- b. Aktifkan Dua Faktor Autentikasi (2FA).
- c. Jangan klik link sembarangan.





CYBERSECURITY AWARENESS

1. KEAMANAN AKUN

Keamanan akun adalah upaya untuk melindungi akun digital pribadi dan dinas dari akses yang tidak sah oleh pihak yang tidak berwenang. Akun digital dapat berupa email, media sosial, akun perbankan, dan lainnya.

PENGGUNAAN PASSWORD KUAT

Password adalah lapisan pertama pertahanan.

- a. Minimal 12 karakter
- b. Kombinasi huruf besar, kecil, tanda baca, dan angka.
- c. Tidak menggunakan informasi pribadi.

CONTOH PASSWORD KUAT

DWRX#1337_AsIFx@





CYBERSECURITY AWARENESS

2. KEAMANAN DATA

Keamanan data adalah upaya untuk melindungi data dari akses, penggunaan, pengungkapan, perubahan, atau penghancuran oleh pihak yang tidak berwenang, baik secara sengaja maupun tidak sengaja.

JENIS DATA YANG HARUS DILINDUNGI

DATA PRIBADI:

- Nomor KTP, KK, Data Rekening, dan Password.

DATA SENSITIF ORGANISASI:

- Data Anggota, Dokumen Rahasia, Informasi Pribadi dan Dinas.

CONTOH ANCAMAN NYATA

- Insider Threat (Orang Dalam).
- Serangan Ransomware, Malware, dan Phising.
- Peretasan Akun





CYBERSECURITY AWARENESS

3. PERAN PENGGUNA

Peran pengguna adalah tanggung jawab setiap individu yang menggunakan sistem atau perangkat pribadi maupun dinas untuk menjaga keamanan data dan mencegah terjadinya ancaman siber.

TANGGUNG JAWAB PENGGUNA

MENJAGA KERAHASIAAN:

- Tidak membagikan password kepada orang lain.
- Tidak menyimpan data sensitif organisasi.
- Tidak mudah percaya dengan orang lain



PENGINGAT

Pengguna bukan hanya sebagai pemakai sistem, tetapi juga sebagai garis pertahanan pertama (First Line of Defense) dalam melindungi informasi.



CYBERSECURITY AWARENESS

4. TANAMKAN MINDSET ZERO TRUST

Dalam lingkungan siber, TNI mulai menerapkan prinsip *Zero Trust*, yaitu pendekatan keamanan yang menekankan sikap kewaspadaan menyeluruh terhadap setiap akses dan permintaan informasi. Prinsip dasarnya sederhana: "*Never Trust, Always Verify*", jangan pernah langsung percaya, dan selalu lakukan verifikasi.



a. Jangan Menganggap Semua Aman

Tidak ada pengguna, perangkat, atau pesan yang boleh langsung dipercaya, meskipun terlihat berasal dari jaringan internal atau dari atasan sendiri.



b. Selalu Verifikasi Melalui Jalur Resmi

Setiap instruksi atau permintaan data yang diterima melalui media digital harus dikonfirmasi ulang melalui saluran komunikasi kedinasan yang sah sebelum ditindaklanjuti.



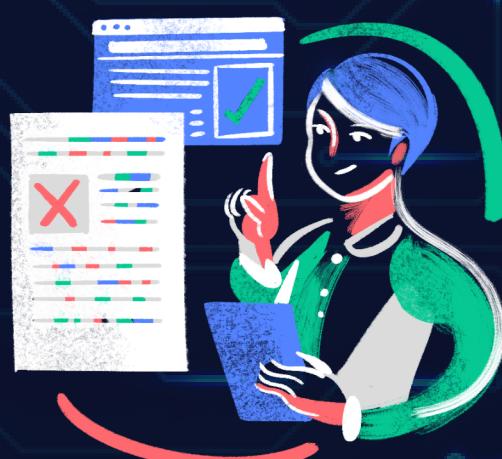
c. Waspadai Rekayasa Sosial (*Social Engineering*)

Pelaku serangan siber sering menyamar sebagai pihak yang dikenal untuk memanfaatkan rasa percaya. Karena itu, sikap kritis dan kebiasaan memverifikasi adalah bagian penting dari disiplin keamanan siber.



KETAHANAN INFORMASI

- 1. Pengertian**
- 2. Ancaman Utama**
- 3. Upaya Peningkatan**
- 4. Manfaat**
- 5. Siap Tanggap & Waspada**

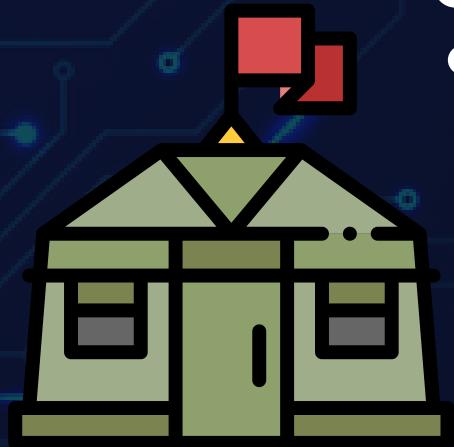




KETAHANAN INFORMASI

1. PENGERTIAN

Ketahanan informasi adalah upaya terintegrasi untuk melindungi kerahasiaan, keutuhan, dan ketersediaan informasi sebagai aset strategis organisasi.





KETAHANAN INFORMASI

2. ANCAMAN UTAMA



Ancaman siber terus berkembang dan menargetkan sistem, data, serta personel sebagai titik lemah organisasi.

- **Serangan Siber**
(hacker, malware, ransomware)
- **Disinformasi dan Hoaks**
Penyebaran informasi palsu untuk memanipulasi opini.
- **Phishing & Pencurian Identitas**
Upaya memperoleh data sensitif melalui rekayasa sosial.
- **Kebocoran Data Pribadi**
Akses atau distribusi data tanpa izin.





KETAHANAN INFORMASI

3. UPAYA PENINGKATAN

Peningkatan ketahanan informasi dilakukan melalui langkah preventif dan penguatan sistem keamanan.



1. Meningkatkan literasi digital personel
2. Menerapkan enkripsi pada data sensitif
3. Memperkuat sistem dan infrastruktur keamanan
4. Menerapkan verifikasi identitas dan autentikasi multi-faktor (MFA)





KETAHANAN INFORMASI

4. MANFAAT



Penerapan ketahanan informasi memberikan dampak langsung terhadap keamanan organisasi dan kepentingan nasional.

- 1. Melindungi data pribadi dan informasi rahasia
- 2. Mencegah penyebaran hoaks dan disinformasi
- 3. Mengurangi risiko kebocoran dan penyalahgunaan data
- 4. Mendukung stabilitas dan keamanan nasional



KETAHANAN INFORMASI

5. SIAP TANGGAP & WASPADA



Setiap personel wajib memiliki kewaspadaan dan kesiapsiagaan terhadap potensi ancaman informasi.

- Tingkatkan kewaspadaan terhadap serangan siber
- Verifikasi kebenaran sebelum menyebarkan informasi
- Hindari provokasi dan penyebaran informasi yang belum terkonfirmasi

Apabila terdapat indikasi ancaman siber atau kerentanan keamanan informasi, segera hubungi kontak resmi Satsiberau di bawah ini.



+62 822-9529-8226



idaf-csirt@tni-au.mil.id



@satsiberau



ETIKA MEDIA SOSIAL

- 1. Memahami Data Pribadi**
- 2. Lindungi Diri di Media Sosial**
- 3. Berpikir Sebelum Posting**
- 4. Memahami Jejak Digital**
- 5. Benteng Kognitif Prajurit:
“Saring Sebelum Sharing”**



TNI AU  **AMPUH**
Adaptif-Modern-Profesional-Unggul-Humanis



18

ETIKA MEDIA SOSIAL

1. MEMAHAMI DATA PRIBADI

Data Pribadi adalah aset strategis bagi prajurit TNI AU



Berhati-hati! **Data bocor** bisa disalahgunakan untuk **spionase dan kejahatan!**

Data Pribadi Umum

1. Nama
2. Jenis Kelamin
3. Status Perkawinan
4. Alamat IP & No. HP



Data Pribadi Spesifik

- Info Kesehatan
- Data Biometrik
- Data Keuangan
- Info Keluarga



Kombinasi data umum tetap berbahaya!

Lindungi Data Pribadi Anda

Jangan unggah data diri atau foto dinas!

Gunakan password kuat & aktifkan verifikasi 2 langkah!

Waspadai link mencurigakan & phising!

Periksa ulang setelan privasi gadget & akun!



19

ETIKA MEDIA SOSIAL

2. LINDUNGI DIRI DI MEDIA SOSIAL

Optimalkan Pengaturan Privasi Akun



Aktifkan “Akun Privat” di semua media sosial



Aktifkan “Akun Privat” di semua media sosial

Batasi akses postingan hanya untuk teman dekat
(Close Friends)

Nonaktifkan pencarian profil via nomor telepon atau email

Gunakan Autentikasi Dua Faktor (2FA)



Platform	Metode 2FA	Cara Aktivasi
Instagram	Aplikasi Auth. / WhatsApp	Pengaturan → Keamanan → 2FA
Tiktok	Email / Aplikasi Authenticator	Pengaturan → Keamanan → 2FA
Facebook	Aplikasi Authenticator	Pusat Akun → Keamanan → 2FA
X	Aplikasi Authenticator	Pengaturan → Keamanan → 2FA

Selalu Waspada!!!

Jangan asal terima permintaan pertemanan atau mengklik link mencurigakan





20

ETIKA MEDIA SOSIAL

3. BERPIKIR SEBELUM POSTING



Verifikasi Informasi dan Penangkalan Hoaks

Cek fakta sebelum membagikan konten apapun:



CEK SUMBER

Pastikan berita berasal dari media massa yang kredibel atau kanal resmi

PERIKSA KEASLIAN VISUAL

Periksa manipulasi digital atau konteks yang keliru (kejadian lama yang diposting baru)



PASTIKAN INFORMASI VALID SEBELUM DISEBAR



Penghormatan terhadap privasi dan hak orang lain

DILARANG!!!

Foto/video kejadian sensitif tanpa izin, terutama di area dinas / sensitif (Alutsista, SOC, Obvitnas, dsb.).



Periksa keaslian visual sebelum ikut menyebarkan.

Curhat masalah **kedinasan** atau gesekan dengan rekan kerja di media sosial.



Standarisasi bahasa dan wibawa prajurit

Komunikatif solutif dan **sopan**

Memviralkan kejadian sensitif itu tidak etis.

Jaga komentar guna menghindari perselisihan dan amplifikasi negatif.



21

ETIKA MEDIA SOSIAL

4. MEMAHAMI JEJAK DIGITAL

Setiap aktivitas online prajurit TNI AU meninggalkan **jejak digital** yang bersifat **permanen**. Jejak ini merupakan **rekaman** yang bisa **ditemukan di masa depan** dan berpengaruh pada **karier serta reputasi di dunia nyata**.



Apa itu Jejak Digital?

Jejak digital adalah jejak permanen aktivitas online yang tersimpan di internet, termasuk:

- Like atau komentar di media sosial
- Foto/video yang diunggah
- Riwayat chat & panggilan telepon
- Rahasia Obrolan Bocor Pesan pribadi atau grup tertutup bisa **disebarluaskan** oleh pihak lain
- Arsip Dijadikan Bukti Komentar & kiriman lama dapat **dipermasalahkan** dalam sidang disiplin/pidana



Jangan pernah tulis/unggah hal yang **Anda tidak ingin dilihat pimpinan atau publik!**



22

ETIKA MEDIA SOSIAL

5. BENTENG KOGNITIF PRAJURIT: "SARING SEBELUM SHARING"

Jangan Latah Berkomentar

Jangan mudah terpancing oleh isu-isu provokatif yang beredar di grup WhatsApp atau media sosial.

1

2

Cek Fakta

Tahan jari Anda. Jika menerima berita yang sensasional atau instruksi tidak lazim, tanyakan kebenarannya kepada rantai komando atau institusi resmi.

Putus Rantai Hoaks

Jika sebuah informasi terbukti palsu atau dirancang untuk memecah belah solidaritas (terutama terkait isu SARA atau netralitas TNI), jangan sebarkan pesan tersebut. Cukup berhenti di Anda.

3



23

PELANGGARAN DAN ANCAMAN HUKUM

01

UU KEBOCORAN DATA INTELIJEN

Pembocoran data intelijen diatur secara spesifik dalam UU No. 17 Th. 2011 Pasal 44 tentang Intelijen Negara: mengatur sanksi pidana penjara maksimal 10 tahun dan denda hingga Rp500 juta bagi setiap orang yang sengaja mencuri, membuka, atau membocorkan Rahasia Intelijen.

02

UU ITE PENYEBARAN INFO RAHASIA

Pasal 32 UU ITE (Perubahan UU ITE No. 1/2024): Melarang dengan sengaja dan tanpa hak atau melawan hukum melakukan transmisi, pemindahan, atau merusak informasi/dokumen elektronik, termasuk yang bersifat rahasia, sehingga dapat diakses oleh publik dengan ancaman 8-10 th penjara serta denda maksimal 5 miliar.

03

PENGINGAT

Setiap personel wajib kerahasiaan informasi klasifikasinya dan membagikannya melalui perangkat pribadi dan dinas.

menjaga sesuai tidak media,



24



PENUTUP

Segenap Prajurit dan ASN TNI AU kebanggaan bangsa Indonesia, jagalah nama baik saudara-saudara, jangan sampai ternoda oleh perbuatan tercela. Suramnya nama saudara akibat perbuatan tercela, mencemarkan Angkatan Udara dan menyuramkan bangsa.

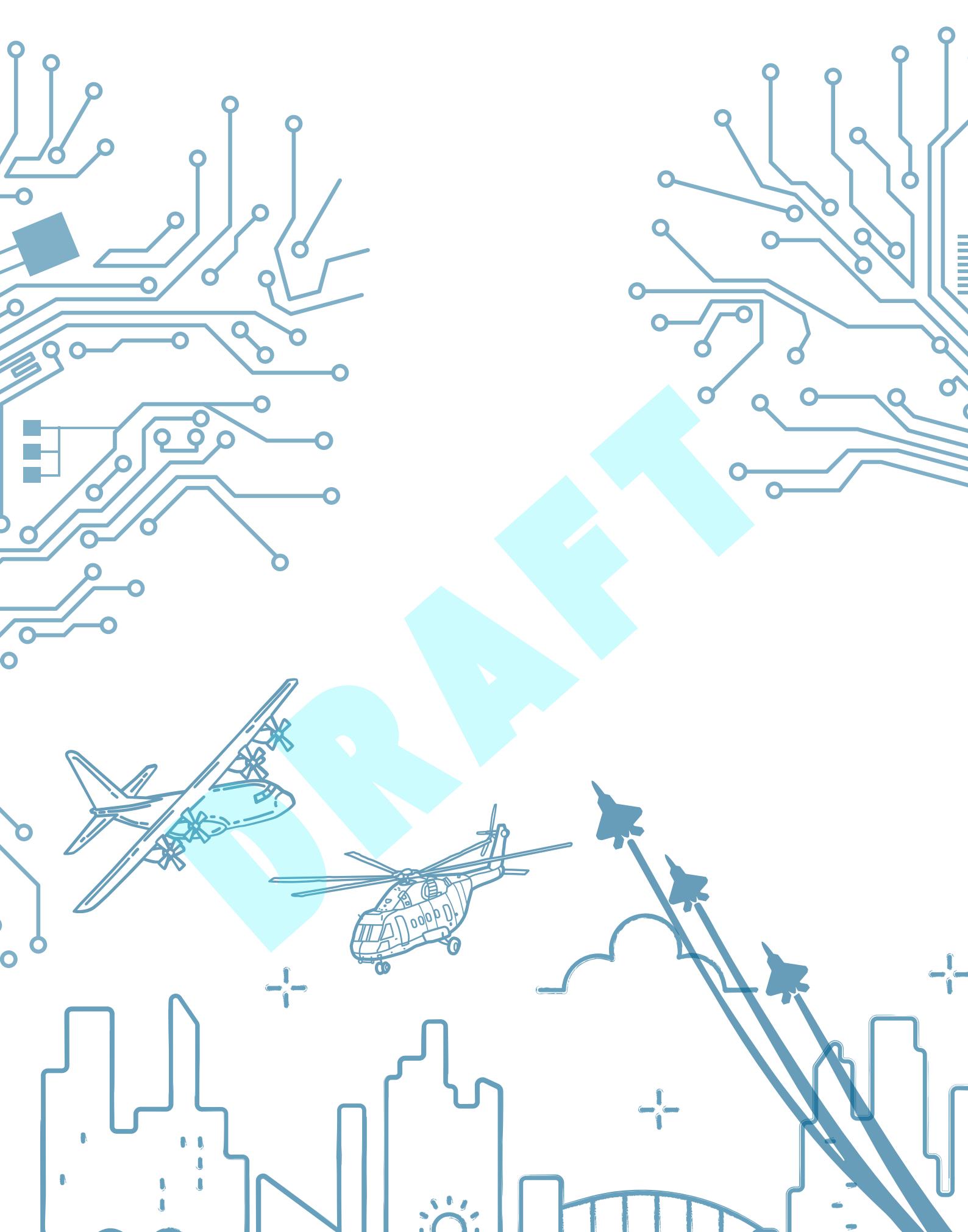
Sementara, perbuatan baik saudara-saudara akan membawa kejayaan Angkatan Udara dan mengharumkan bangsa Indonesia

Kepala Staf Angkatan Udara

Marsekal TNI M. Tonny Harjono, S.E., M.M.

BUKU SAKU TIGA PILAR KETAHANAN INFORMASI

TNI AU **AMPUH**
Adaptif-Modern-Profesional-Unggul-Humanis



BUKU SAKU TIGA PILAR KETAHANAN INFORMASI

TNI AU  **AMPUH**

Adaptif-Modern-Profesional-Unggul-Humanis

TNI AU AMPUH
Adaptif-Modern-Profesional-Unggul-Humanis