

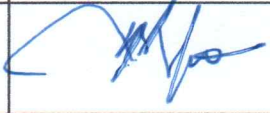



	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 1


**DOKUMEN DIREKTORAT PENGEMBANGAN  
TEKNOLOGI INFORMASI  
UNIVERSITAS BHAYANGKARA JAKARTA RAYA**

<b>KEBIJAKAN KEAMANAN INFORMASI UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>				
No	Nama	Jabatan	Status	Tanda Tangan
1.	Arif Rifai Dwiyanto, S.T., M.T.I.	Pjs. Ses. Dir. PTI & PoC CSIRT Ubhara Jaya	Merumuskan	
2.	Nurfiyah, S.T., M.Kom	Pjs. Kasubdit Tata Kelola Direktorat PTI	Merumuskan	
3.	Dani Yusuf, M.Kom	Plt. Dir. PTI & Ketua CSIRT Ubhara Jaya	Memvalidasi	
4.	Dr. Zahara Tussoleha Rony, S.Pd., M.M	Wakil Rektor IV	Menyetujui	
5.	Irjen Pol. (Purn) Prof. Dr. Drs. H. Bambang Karsono, S.H., M.M	Rektor	Menyetujui	

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 2

## DAFTAR ISI

1. Kebijakan dan Cakupan Sistem Informasi Manajemen	3
2. Standar Penerapan Sistem Manajemen Keamanan Informasi	4
3. Manajemen Resiko Keamanan Sistem Informasi	6
4. Tata Kelola Dokumentasi Sistem Manajemen Keamanan Informasi	6
5. Organisasi Keamanan Informasi	7
6. Keamanan Sumber Daya Manusia	8
7. Pengelolaan Aset	8
8. Pengendalian Akses	10
9. Penggunaan Kriptografi	11
10. Pengelolaan Keamanan Fisik dan Lingkungan	11
11. Keamanan Operasional	12
12. Keamanan Informasi	14
13. Akuisisi, Pengembangan dan Pemeliharaan Sistem	14
14. Pengendalian Pihak Ketiga (Vendor/Pemasok dan Provider/ Penyedia)	15
15. Pengelolaan Insiden Keamanan Informasi	16
16. Pengendalian Aspek Keamanan Informasi dalam Kesiambungan Usaha	17
17. Kepatuhan	17
18. Kebijakan <i>Clear Desk - Clear Screen</i>	18

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 3

## 1. Kebijakan dan Cakupan Sistem Informasi Manajemen

### 1.1 Tujuan

Untuk memberikan arahan kepada Civitas Akademika Universitas Bhayangkara Jakarta Raya dan memberikan dukungan terhadap keamanan informasi sesuai dengan kebutuhan Universitas serta hukum dan peraturan yang berlaku.


### 1.2 Penerapan

1.2.1 Universitas Bhayangkara Jakarta Raya memahami bahwa informasi adalah aset yang perlu dilindungi. Oleh karena itu, Universitas Bhayangkara Jakarta Raya berkomitmen untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) sehingga menjamin perlindungan keamanan informasi untuk menjamin kerahasiaan, integritas dan ketersediaan sesuai standar internasional. Untuk mencapai hal tersebut di atas, Universitas Bhayangkara Jakarta Raya menyusun rencana sistem manajemen keamanan informasi di Universitas Bhayangkara Jakarta Raya berdasarkan hal-hal berikut:

- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
- Undang-Undang Republik Indonesia Nomor 12 Tahun 2012, tentang Pendidikan Tinggi.
- Peraturan Menteri Kominfo No.4/2016 tentang Sistem Manajemen Pengamanan Informasi.
- Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Peraturan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 25 Tahun 2018 tentang Perizinan Berusaha Terintegrasi Secara Elektronik Sektor Pendidikan dan Kebudayaan.
- Standar Internasional ISO/IEC 27001 *Information security management systems*.
- Standar Internasional ISO/IEC 29147 *Information technology - Security techniques - Vulnerability disclosure*.
- Hasil Kajian Risiko Keamanan Informasi.
- Kebutuhan internal terhadap pengamanan informasi dengan sudut pandang bahwa informasi adalah aset yang harus dilindungi.
- Peraturan Internal Universitas Bhayangkara Jakarta Raya di antaranya:
  - Peraturan Kepegawaian.
  - Peraturan Akademik.

1.2.2 Untuk mendukung keberhasilan implementasi Sistem Manajemen Keamanan Informasi di Universitas Bhayangkara Jakarta Raya, Universitas Bhayangkara Jakarta Raya telah mengidentifikasi hal-hal sebagai berikut:

- Manajemen harus menetapkan sasaran keamanan informasi tahunan, yang merupakan kesatuan dari sistem manajemen kinerja Universitas Bhayangkara

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 4

Jakarta Raya.

- Memastikan kepatuhan terhadap semua hukum dan peraturan yang berlaku terkait keamanan informasi.
- Memastikan bahwa penilaian risiko keamanan informasi dilakukan secara teratur.
- Memastikan bahwa dokumen pendukung yang diperlukan tersedia setiap saat untuk memenuhi ketentuan kerahasiaan yang tercantum dalam dokumen ini.
- Menyediakan sumber daya yang diperlukan untuk menerapkan sistem manajemen keamanan informasi secara efektif serta memantau pencapaian tujuan keamanan informasi.
- Memastikan pelaksanaan audit internal sistem manajemen keamanan informasi sesuai dengan peraturan yang berlaku.
- Memastikan bahwa tinjauan manajemen terhadap sistem manajemen keamanan informasi dilakukan, minimal setahun sekali.
- Memastikan bahwa perbaikan berkelanjutan dari implementasi sistem manajemen keamanan informasi selalu dilakukan.

#### 1.2.3 Ruang Lingkup Sistem Manajemen Keamanan Informasi:

- Pelaksana: Direktorat Pengembangan Teknologi Informasi (Dit. PTI) dan *Computer Security Incident Response Team* (CSIRT).
- Lokasi : Universitas Bhayangkara Jakarta Raya, Jl. Raya Perjuangan No. 81, Bekasi Utara, Kota Bekasi, Jawa Barat 17142, Indonesia
- Proses bisnis/layanan : Layanan *Network*, Infrastruktur TIK, Aplikasi, dan *Helpdesk*.
- Aset berupa :
  - a. Data dan Informasi,
  - b. Sistem Informasi,
  - c. Sumber Daya Manusia,
  - d. Perangkat Lunak / *Software*,
  - e. Perangkat Keras / *Hardware*,
  - f. Perangkat Jaringan, dan
  - g. Perangkat dan Fasilitas Pendukung.


## 2. Standar Penerapan Sistem Manajemen Keamanan Informasi

### 2.1 Tujuan

Standar ini dimaksudkan untuk memberikan pedoman terhadap penerapan Sistem Manajemen Keamanan Informasi (SMKI) di Universitas Bhayangkara Jakarta Raya dengan menggunakan siklus P - D - C - A ( *Plan - Do - Check - Act* ) yang berdasarkan ISO/IEC 27001 sehingga aset informasi Universitas Bhayangkara Jakarta Raya dapat terlindungi dari aspek Privasi, Kerahasiaan, Integritas dan Ketersediaan yang dimana merupakan faktor penting dalam menjaga keamanan data.

### 2.2 Penerapan

#### 2.2.1 Tahap Proses Perencanaan (*Plan*)

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 5

Tahap Proses Perencanaan (*Plan*), terdiri dari :

- Menentukan isu internal dan eksternal yang dapat mempengaruhi proses implementasi Sistem Informasi Manajemen Keamanan Informasi.
- Menentukan pihak-pihak terkait proses implementasi Sistem Manajemen Keamanan Informasi serta mengidentifikasi persyaratan dan kebutuhan keamanan informasinya.
- Menentukan ruang lingkup penerapan Sistem Manajemen Keamanan Informasi.
- Menetapkan suatu komitmen manajemen terhadap penerapan Sistem Manajemen Keamanan Informasi.
- Mengkomunikasikan dan mensosialisasikan pedoman keamanan informasi.
- Melakukan asesmen risiko keamanan informasi.
- Menyusun Rencana Mitigasi Risiko Keamanan Informasi.
- Menentukan sasaran penerapan Sistem Manajemen Keamanan Informasi.
- Menentukan sumber daya yang diperlukan untuk penerapan Sistem Manajemen Keamanan Informasi.

#### 2.2.2 Tahapan Proses Pelaksanaan (*Do*)

Tahapan Proses Pelaksanaan (*Do*), terdiri dari:

- Menyusun Dokumentasi proses implementasi sistem manajemen keamanan informasi.
- Mengevaluasi risiko keamanan informasi ketika risiko baru ditambahkan atau ketika ada perubahan signifikan yang dapat mempengaruhi keamanan informasi.
- Menerapkan kesadaran dan pelatihan sistem manajemen keamanan informasi.
- Memperoleh dan mengelola sumber daya untuk mendukung penerapan sistem manajemen keamanan informasi.
- Melaksanakan implementasi sistem manajemen keamanan informasi sesuai dengan tujuan (rencana) yang ditetapkan dalam proses perencanaan.

#### 2.2.3 Tahapan Proses Evaluasi (*Check*)

Tahapan Proses Evaluasi (*Check*), terdiri dari :


- Mengevaluasi efektivitas penerapan pengendalian keamanan informasi setidaknya setiap tahun 1 (satu) kali.
- Memantau dan melaporkan pencapaian tujuan sistem manajemen keamanan informasi setidaknya setiap tahun.
- Tinjau hasil penilaian risiko setidaknya setiap enam bulan.
- Melakukan audit internal atas penerapan sistem manajemen keamanan informasi minimal setahun sekali.
- Melakukan tinjauan jajaran manajemen penerapan sistem manajemen keamanan informasi setidaknya setiap tahun.

#### 2.2.4 Tahapan Proses Tindak Lanjut (*Act*)

Tahapan Proses Tindak Lanjut (*Act*), terdiri dari :

- Monitoring pelaksanaan rencana tindakan korektif terhadap hasil audit internal.
- Mengenai pengoperasian sistem manajemen keamanan informasi, kami akan merencanakan ulang setiap tahun dan melakukan perbaikan terus-menerus.



	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 6

### 2.3 Dokumen Pendukung

- Dokumen Rencana Strategis Pengembangan Teknologi Informasi Ubhara Jaya.
- Dokumen *Integrated Management System Plan*.
- Dokumen Laporan Audit Internal dan / atau Eksternal.

## 3. Manajemen Risiko Keamanan Sistem Informasi

### 3.1 Tujuan

Panduan tentang cara melakukan penilaian risiko dan menilai kecukupan risiko keamanan informasi berdasarkan kriteria *Confidentiality*, *Integrity*, dan *Availability* (CIA) yang telah ditetapkan.

### 3.2 Penerapan

3.2.1 Penilaian risiko keamanan informasi secara terencana perlu dilakukan untuk menghadapi prioritas-prioritas usaha yang berubah dan ancaman-ancaman baru terhadap keamanan data dan informasi.


3.2.2 Penilaian risiko keamanan informasi membantu mengidentifikasi risiko-risiko terkait keamanan informasi (*risk register*) dan memungkinkan untuk melakukan mitigasi terhadap risiko tersebut dengan menggunakan memakai pengendalian yang sesuai. Dari hasil evaluasi risiko keamanan informasi dapat dipilih prioritas dan menerapkan pengendalian keamanan informasi dari suatu tingkat risiko yang diterima atau *Acceptable Risk Level* (ARL). Manajemen Sistem Manajemen Keamanan Informasi mengevaluasi kecukupan risiko keamanan informasi yang terdiri dari berbagai kriteria berikut:

- Kendala-kendala Finansial dan Sumber Daya Manusia saat ini,
- Rekomendasi dari berbagai pihak,
- Hasil-hasil audit Sistem Manajemen Keamanan Informasi serta audit sistem informasi, dan
- Kecenderungan insiden keamanan yang terjadi sebelumnya.

3.2.3 Tingkat risiko keamanan informasi yang bisa diterima atau *Acceptable Risk Level* (ARL) wajib dikaji ulang setiap tahun dan digunakan menjadi bagian berdasarkan masukan bagi manajemen risiko. Penyelarasan menggunakan manajemen risiko strategis untuk mengkoordinasikan keputusan risiko jangka panjang dan untuk mitigasi masalah-masalah yang sedang dihadapi.

### 3.3 Dokumen Pendukung

- Dokumen Pedoman Pengelolaan Resiko.
- Dokumen *Risk Register*.
- Dokumen *Acceptable Risk Level* (ARL).

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 7

## 4. Tata Kelola Dokumentasi Sistem Manajemen Keamanan Informasi

### 4.1 Tujuan

- 4.1.1 Mendeskripsikan dan menjabarkan struktur dokumentasi yang diterapkan Universitas Bhayangkara Jakarta Raya.
- 4.1.2 Mengidentifikasi aset teknologi informasi yang digunakan dalam penyelenggaraan layanan Teknologi Informasi Universitas Bhayangkara Jakarta Raya.

### 4.2 Penerapan

Dengan menggunakan peta dokumentasi SMKI, pedoman-pedoman khusus, standar-standar khusus dan prosedur-prosedur khusus diidentifikasi. Penerapan dokumentasi ini adalah khusus untuk lingkungan yang telah ditetapkan.

### 4.3 Dokumen Pendukung

Jenis Dokumen Prosedur Pengendalian Informasi :

Jenis Dokumen	Definisi
<b>Kebijakan</b>	Dokumen kebijakan teknologi informasi di Universitas Bhayangkara Jakarta Raya.
<b>Pedoman</b>	Dokumen yang memberikan pedoman dalam implementasi keamanan informasi
<b>Standar</b>	Dokumen yang berisi persyaratan minimum dan ditetapkan berdasarkan konsensus para pemangku kepentingan dalam implementasi keamanan informasi
<b>Prosedur</b>	Dokumen yang berisi tata cara untuk menjalankan proses implementasi keamanan informasi
<b>Formulir</b>	Dokumen untuk merekam semua kegiatan implementasi keamanan informasi agar hasilnya dapat didokumentasikan


## 5. Organisasi Keamanan Informasi

### 5.1 Tujuan

Membuat kerangka kerja manajemen untuk memulai dan mengendalikan serta mengimplementasi keamanan informasi dan proses operasional dalam organisasi.

### 5.2 Penerapan

- 5.2.1 Semua tanggung jawab keamanan informasi harus dijabarkan, ditetapkan dan dialokasikan.
- 5.2.2 Memisahkan tugas dan tanggung jawab yang saling bertentangan untuk mengurangi peluang perubahan yang tidak sah atau tidak disengaja dan penyalahgunaan aset teknologi informasi.
- 5.2.3 Mengidentifikasi dan terlibat dengan komunitas keamanan informasi.
- 5.2.4 Pengendalian keamanan informasi harus diterapkan dalam manajemen proyek dan diterapkan pada semua tahapan metodologi manajemen proyek.

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 8

### 5.3 Dokumen Pendukung

- Surat Keputusan Pembentukan CSIRT Ubhara Jaya.
- Dokumen Struktur Organisasi dan Tata Kerja CSIRT.
- Dokumen Deskripsi Kerja/*Job Description* CSIRT.
- Bukti kerja sama dengan pihak berwenang dan/atau keikutsertaan dalam komunitas keamanan informasi nasional/internasional.

## 6. Keamanan Sumber Daya Manusia

### 6.1 Tujuan

- 6.1.1 Memastikan bahwa karyawan dan Pegawai Harian Lepas (PHL) memahami peran dan tanggung jawab pekerjaan mereka dan cocok untuk peran dan tanggung jawab tersebut.
- 6.1.2 Memastikan karyawan dan Pegawai Harian Lepas (PHL) memahami dan menerapkan peran dan tanggung jawab keamanan informasi mereka.
- 6.1.3 Melindungi kepentingan Universitas sehubungan dengan prosedur rekrutmen, perubahan/mutasi dan pemutusan hubungan kerja.


### 6.2 Penerapan

- 6.2.1 Pemeriksaan latar belakang pada semua calon karyawan dan Pegawai Harian Lepas (PHL) Universitas Bhayangkara Jakarta Raya harus dilakukan sesuai dengan hukum, peraturan, dan etika yang berlaku.
- 6.2.2 Kontrak dengan karyawan dan Pegawai Harian Lepas (PHL) Universitas Bhayangkara Jakarta Raya harus memperjelas peran dan tanggung jawab keamanan informasi.
- 6.2.3 Manajemen harus mewajibkan semua karyawan dan Pegawai Harian Lepas (PHL) Universitas Bhayangkara Jakarta Raya untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur dalam organisasi.
- 6.2.4 Seluruh karyawan dan Pegawai Harian Lepas (PHL) Universitas Bhayangkara Jakarta Raya wajib mendapatkan pendidikan, sosialisasi dan pelatihan keamanan informasi sesuai dengan tanggung jawab pekerjaannya.
- 6.2.5 Pemberian sanksi formal harus dikomunikasikan serta konsisten dengan kebijakan dan prosedur organisasi, harus ada untuk mengambil tindakan terhadap karyawan yang melakukan pelanggaran keamanan informasi.
- 6.2.6 Peran dan tanggung jawab keamanan informasi harus terus berlaku jika terjadi perubahan atau pemutusan hubungan kerja.

### 6.3 Dokumen Pendukung

- Surat Keterangan Catatan Kepolisian (SKCK).
- Dokumen *Non-Disclosure Agreement* (NDA) Pegawai dan Pihak Ketiga.
- Dokumen Laporan Pelatihan/*Training* Pegawai.
- Dokumen Hasil Evaluasi Kinerja Pegawai.



	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 9

## 7. Pengelolaan Aset


### 7.1 Tujuan

- 7.1.1 Untuk mengidentifikasi aset Universitas Bhayangkara Jakarta Raya dan menetapkan tanggung jawab untuk perlindungan yang tepat dari aset tersebut.
- 7.1.2 Untuk memastikan keamanan informasi tepat guna dengan tingkat kepentingan informasi.
- 7.1.3 Mencegah kebocoran, modifikasi, penghapusan, dan penghancuran informasi yang disimpan oleh pihak yang tidak bertanggungjawab.

### 7.2 Penerapan

- 7.2.1 Aset terkait dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan diinventarisasi secara berkala.
- 7.2.2 Pemilik aset Teknologi Informasi bertanggung jawab untuk menetapkan dan menerapkan kontrol keamanan untuk aset Teknologi Informasi yang mereka kelola dan melindunginya dari berbagai aspek ancaman terhadap kerahasiaan, integritas, dan ketersediaan sepanjang masa berlakunya.
- 7.2.3 Aturan diterapkan terhadap penggunaan informasi dan aset.
- 7.2.4 Semua karyawan dan pengguna eksternal harus mengembalikan semua aset yang dimiliki dan digunakan oleh Universitas Bhayangkara Jakarta Raya pada saat pemutusan hubungan kerja, kontrak atau perjanjian.
- 7.2.5 Aset informasi dikategorikan berdasarkan tingkat kerahasiaan, nilai, tingkat kritikalitas, dan aspek hukum.

Klasifikasi	Definisi
<b>Rahasia</b>	<p>Informasi yang membutuhkan pengamanan tinggi/ketat dan hanya boleh diketahui oleh pimpinan dan/atau personil tertentu yang ditetapkan.</p> <p>Pembocoran informasi ini secara tidak berwenang dapat menimbulkan risiko yang TINGGI/BESAR bagi Universitas Bhayangkara Jakarta Raya, seperti antara lain:</p> <ul style="list-style-type: none"> <li>– kehilangan reputasi;</li> <li>– ketidakpatuhan terhadap regulasi;</li> <li>– kerugian finansial yang besar; atau</li> <li>– terganggunya layanan Teknologi Informasi dalam jangka lama.</li> </ul> <p>Jenis informasi yang termasuk klasifikasi ini antara lain: Topologi jaringan dengan IP Address, hasil <i>penetration test</i>, hasil penilaian kinerja karyawan, <i>log system administrator</i>, dan informasi rahasia lainnya.</p>

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : <b>10</b>

<b>Terbatas</b>	<p>Informasi yang telah terdistribusi di lingkungan internal Universitas Bhayangkara Jakarta Raya yang penyebarannya secara internal tidak memerlukan persetujuan dari pemilik informasi. Risiko kebocoran informasi secara tak berwenang ke pihak luar berkategori SEDANG/MENENGAH, tidak sebesar risiko informasi berklasifikasi “Rahasia”</p> <p>Jenis informasi yang termasuk klasifikasi ini antara lain: Kebijakan dan prosedur, laporan audit (internal/eksternal), hasil kajian risiko, risalah rapat internal dan laporan operasional layanan Teknologi Informasi.</p>
-----------------	---

- 7.2.6 Identifikasi klasifikasi aset informasi harus seragam dan menyeluruh untuk semua aset informasi.
- 7.2.7 Aset informasi harus dikelola sesuai dengan skema klasifikasi informasi yang diadopsi.
- 7.2.8 Tetapkan aturan untuk mengelola media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi.
- 7.2.9 Media penyimpan informasi harus dibuang/dimusnahkan secara aman bila tidak diperlukan lagi.
- 7.2.10 Pengiriman media penyimpanan data yang berisi informasi harus dilindungi dari akses yang tidak sah dan penyalahgunaan selama proses pengiriman.

### 7.3 Dokumen Pendukung

- Pengelolaan Aset Informasi dan Klasifikasi Informasi.


## 8. Pengendalian Akses

### 8.1 Tujuan

- 8.1.1 Membatasi akses terhadap informasi dan perangkat pemrosesan informasi.
- 8.1.2 Memastikan hanya pengguna yang berwenang dan mencegah pihak yang tidak berwenang masuk ke dalam sistem dan layanan.
- 8.1.3 Memastikan pengguna bertanggung jawab dalam menjaga otentikasi terhadap informasi.
- 8.1.4 Memastikan dan mencegah adanya akses secara tidak berwenang terhadap informasi dan fasilitas sistem informasi baik aplikasi, sistem operasi, internet dan akses ruang server/data center.

### 8.2 Penerapan

- 8.2.1 Sebuah aturan terkait pengendalian akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan usaha dan informasi.
- 8.2.2 Pengguna hanya boleh diizinkan mengakses layanan jaringan dan jaringan yang secara khusus diizinkan untuk mereka gunakan.
- 8.2.3 Diterapkan proses pendaftaran dan penghapusan akun pengguna.

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : <b>11</b>

- 8.2.4 Proses penyediaan akses pengguna ke sumber daya informasi harus berlaku untuk semua jenis pengguna untuk semua sistem dan layanan.
- 8.2.5 Pemberian dan penggunaan hak akses khusus harus dibatasi dan dikendalikan.
- 8.2.6 Penetapan kredensial sensitif (seperti kata sandi) harus dikontrol melalui proses secara formal.
- 8.2.7 Pemilik aset harus melakukan pengecekan hak akses pengguna secara berkala.
- 8.2.8 Semua akses karyawan dan pengguna eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan hubungan kerja, kontrak, atau perjanjian.
- 8.2.9 Pengguna harus mematuhi peraturan mengenai penggunaan kredensial sensitif (seperti kata sandi).
- 8.2.10 Akses ke sistem informasi dan aplikasi harus dibatasi sesuai dengan aturan kontrol akses yang berlaku.
- 8.2.11 Akses ke sistem dan aplikasi harus dikontrol menggunakan metode *log in* yang aman.
- 8.2.12 Mekanisme manajemen kata sandi harus interaktif dan memastikan kata sandi berkualitas tinggi.
- 8.2.13 Penggunaan utilitas/alat yang dapat mengesampingkan sistem atau aplikasi harus dibatasi dan dikontrol secara ketat.
- 8.2.14 Akses ke *source code* program harus dibatasi.
- 8.2.15 Hak akses logis dan fisik (pusat data, pusat jaringan, dan semua ruang staf administrasi pusat Teknologi Informasi) ditetapkan secara terbatas sesuai dengan tugas utama dan hak istimewa pengguna. Pemberian akses, tentu saja, membutuhkan setidaknya persetujuan dari kepala departemen yang bertanggung jawab.
- 8.2.16 Akses Tingkat Tinggi seperti Admin hanya digunakan untuk aktivitas yang membutuhkan *user* admin. Akses administrator tidak digunakan untuk melakukan tugas operasional, sehingga pegawai yang memiliki Hak Akses Administrator terbatas.

### 8.3 Dokumen Pendukung

- Matriks Hak Akses.
- Kebijakan Keamanan Infrastruktur.


## 9. Penggunaan Kriptografi

### 9.1 Tujuan

Tujuannya adalah untuk memastikan penggunaan yang tepat dan efektif terhadap kriptografi untuk melindungi kerahasiaan, keabsahan, dan integritas dari informasi.

### 9.2 Penerapan

- 9.2.1 Standar mengenai penggunaan kontrol kriptografi untuk melindungi informasi harus dikembangkan dan diterapkan.
- 9.2.2 Menetapkan dan memberlakukan standar untuk penggunaan dan perlindungan

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 12

kunci kriptografi.

### 9.3 Dokumen Pendukung

- Bukti enkripsi pada aplikasi / trafik data.


## 10. Pengelolaan Keamanan Fisik dan Lingkungan

### 10.1 Tujuan

- 10.1.1 Untuk mencegah akses yang tidak sah, kerusakan, atau gangguan terhadap informasi dan peralatan pemrosesan informasi Universitas Bhayangkara Jakarta Raya.
- 10.1.2 Mencegah kehilangan, kerusakan, pencurian, atau terjadinya segala sesuatu yang dapat membahayakan harta benda Universitas Bhayangkara Jakarta Raya dan mengganggu operasionalnya.

### 10.2 Penerapan

- 10.2.1 Parameter keamanan harus ditetapkan dan digunakan untuk melindungi daerah-daerah yang berisi informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.
- 10.2.2 Area aman harus dilindungi oleh kontrol masuk yang tepat untuk menjamin bahwa hanya personil berwenang yang diperbolehkan untuk mengakses.
- 10.2.3 Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.
- 10.2.4 Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dirancang dan diterapkan.
- 10.2.5 Aturan untuk bekerja di area aman harus dirancang dan diterapkan.
- 10.2.6 Jalur akses seperti area pengiriman dan area bongkar muat di mana orang yang tidak berwenang bisa memasuki tempat tersebut harus dikendalikan
- 10.2.7 Peralatan harus diletakkan dan dilindungi untuk mengurangi risiko dari ancaman lingkungan dan bahaya, dan kesempatan terhadap akses oleh yang tidak berwenang.
- 10.2.8 Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam fasilitas pendukung.
- 10.2.9 Kabel daya dan kabel telekomunikasi maupun jaringan *wireless* yang dilalui data harus dilindungi dari intersepsi, gangguan atau kerusakan.
- 10.2.10 Peralatan harus dipelihara dengan benar untuk memastikan aspek ketersediaan dan integritas.
- 10.2.11 Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin sebelumnya.
- 10.2.12 Keamanan harus diterapkan untuk aset yang berada diluar lokasi dengan memperhitungkan risiko yang berbeda dari bekerja di luar tempat instansi.
- 10.2.13 Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa secara aman sebelum dibuang atau digunakan kembali
- 10.2.14 Pengguna harus memastikan bahwa perangkat pengolah informasi yang ditinggal

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 13

tanpa pengawasan memiliki perlindungan dari akses yang tidak berwenang.

10.2.15 Menetapkan aturan mengenai kebersihan area kerja dari dokumen kertas dan media penyimpanan *removable* dan fasilitas pengolahan informasi.

### 10.3 Dokumen Pendukung

- Peta *Physical Security Area*.
- *Access Log*.
- Ketentuan Ruang Kerja.

## 11. Keamanan Operasional


### 11.1 Tujuan

- 11.1.1 Memastikan proses operasional terhadap perangkat pemrosesan informasi sesuai dengan standar prosedur yang berlaku.
- 11.1.2 Memastikan perangkat pemrosesan informasi terlindungi dari ancaman *malware* (virus, trojan, *ransomware*, dll).
- 11.1.3 Melindungi dari kehilangan data.
- 11.1.4 Merekam *event* atau *log* pada perangkat pengolahan informasi.
- 11.1.5 Memastikan sistem informasi terintegrasi secara keseluruhan.
- 11.1.6 Mencegah penyalahgunaan terhadap kerentanan teknis.
- 11.1.7 Meminimalkan dampak aktivitas audit pada sistem informasi.
- 11.1.8 Memastikan keamanan terhadap pengguna yang melakukan Pembelajaran Jarak Jauh (PJJ), *Work From Home/WFH* atau *remote worker* dan *mobile device*.

### 11.2 Penerapan

- 11.2.1 Prosedur operasional harus didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.
- 11.2.2 Mengendalikan perubahan terhadap proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi.
- 11.2.3 Penggunaan sumber daya harus dimonitor, dievaluasi dan diproyeksikan dari kebutuhan kapasitas di masa depan untuk memastikan kebutuhan kinerja sistem.
- 11.2.4 Pengembangan, pengujian, dan operasional lingkungan harus dipisahkan untuk mengurangi risiko perubahan lingkungan operasional.
- 11.2.5 Pengendalian terhadap deteksi, pencegahan, dan pemulihan untuk melindungi dari *malware* harus diterapkan.
- 11.2.6 Salinan cadangan atau *back-up* informasi, perangkat lunak, dan gambar sistem harus di *manage* dan diuji secara teratur sesuai dengan peraturan yang disepakati.
- 11.2.7 Menerapkan *Event Log* yang berfungsi untuk merekam kegiatan pengguna dan kejadian keamanan informasi pada perangkat Teknologi Informasi.
- 11.2.8 Fasilitas informasi *log* harus dilindungi terhadap gangguan dan akses yang tidak berwenang.
- 11.2.9 Operator dan administrator sistem harus tercatat (*logged*) pada sistem dan catatan (*log*) tersebut harus dilindungi dan dikaji secara berkala.
- 11.2.10 Penunjuk jam (waktu) dari semua sistem pengolahan informasi harus



	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 14

disinkronisasikan sesuai referensi sumber waktu tunggal.

- 11.2.11 Instalasi perangkat lunak pada sistem operasional dan instalasi yang dilakukan oleh pengguna harus diterapkan sesuai peraturan.
- 11.2.12 Informasi mengenai kerentanan teknis dalam sistem informasi harus diperoleh tepat waktu, penjabaran kerentanan tersebut harus dinilai, dan dilakukan tindakan segera mungkin untuk mengatasi risiko yang tidak diinginkan.
- 11.2.13 Audit yang dilakukan pada sistem informasi harus direncanakan dan disetujui secara hati-hati untuk meminimalkan gangguan terhadap proses bisnis.
- 11.2.14 Aturan harus ditetapkan untuk mengelola risiko yang ditimbulkan oleh penggunaan perangkat seluler.
- 11.2.15 Sebuah aturan harus ditetapkan untuk melindungi informasi yang diakses, diproses atau disimpan pada perangkat *teleworking*.

### 11.3 Dokumen Pendukung

- Aplikasi *Configuration Management*.
- Laporan Performansi per semester.
- *Capacity Plan*.
- Laporan pengujian *backup* dan *restore*.
- Peraturan penggunaan *mobile device* dan perangkat *teleworking*.


## 12. Keamanan Informasi

### 12.1 Tujuan

- 12.1.1 Memastikan perlindungan dan dukungan terhadap perangkat pemrosesan informasi di dalam jaringan.
- 12.1.2 Menjaga keamanan terhadap informasi yang dipertukarkan di lingkungan Universitas Bhayangkara Jakarta Raya maupun yang dipertukarkan di luar lingkungan Universitas Bhayangkara Jakarta Raya.

### 12.2 Penerapan

- 12.2.1 Jaringan harus dikelola dan dikendalikan untuk melindungi informasi yang berada dalam sistem dan aplikasi.
- 12.2.2 Mekanisme keamanan, tingkat layanan, dan persyaratan manajemen untuk semua layanan jaringan harus diidentifikasi dan disertakan dalam perjanjian layanan jaringan. Ini terlepas dari apakah layanan ini disediakan secara internal atau menggunakan layanan pihak vendor/provider.
- 12.2.3 Layanan informasi, pengguna dan sistem informasi di dalam jaringan harus dilakukan pada grup terpisah.
- 12.2.4 Peraturan mengenai pengalihan informasi harus ditetapkan untuk melindungi pengalihan informasi melalui penggunaan semua jenis fasilitas komunikasi.
- 12.2.5 Perjanjian antara Universitas Bhayangkara Jakarta Raya dan pihak luar harus membahas tentang pengalihan yang aman terhadap informasi.
- 12.2.6 Informasi yang terlibat dalam pesan elektronik harus dilindungi secara tepat.
- 12.2.7 Persyaratan perjanjian kerahasiaan atau kerahasiaan yang mencerminkan

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : <b>15</b>

persyaratan perlindungan informasi internal Universitas Bhayangkara Jakarta Raya harus diidentifikasi, ditinjau secara berkala, dan didokumentasikan.

### 12.3 Dokumen Pendukung

- Topologi Jaringan.
- *Service Level Agreement* (SLA).
- *Non-Disclosure Agreement* (NDA) dengan Pihak Ketiga.


## 13. Akuisisi, Pengembangan dan Pemeliharaan Sistem

### 13.1 Tujuan

- 13.1.1 Memastikan keamanan informasi adalah bagian yang tidak terpisahkan dari siklus hidup sistem informasi. Hal ini juga mencakup kebutuhan sistem informasi yang menyediakan layanan melalui jaringan publik.
- 13.1.2 Memastikan keamanan informasi dibuat dan diterapkan dalam siklus pengembangan sistem informasi.
- 13.1.3 Memastikan perlindungan terhadap data yang digunakan untuk pengujian (*testing*).

### 13.2 Penerapan

- 13.2.1 Kebutuhan mengenai keamanan informasi harus diselipkan dalam persyaratan untuk perancangan sistem informasi yang baru atau ditambahkan pada sistem informasi yang sedang berjalan.
- 13.2.2 Melindungi kegiatan kecurangan, pengungkapan yang tidak sah serta kegiatan modifikasi Informasi yang ada pada layanan aplikasi yang melewati jaringan publik.
- 13.2.3 Melindungi Informasi yang terlibat dalam transaksi layanan aplikasi agar mencegah transmisi data yang tidak lengkap, *mis-routing*, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan yang tidak sah.
- 13.2.4 Menerapkan peraturan untuk pengembangan sistem dan perangkat lunak untuk proses pengembangan di dalam institusi.
- 13.2.5 Perubahan terhadap sistem dalam siklus pengembangan harus menggunakan prosedur perubahan yang formal.
- 13.2.6 Apabila terjadi perubahan *platform*/sistem operasi, aplikasi yang penting harus ditinjau dan diuji untuk memastikan bahwa tidak ada dampak buruk dari perubahan tersebut terhadap keamanan informasi.
- 13.2.7 Modifikasi terhadap paket perangkat lunak (*software package*) harus diminimalkan, dan semua perubahan harus dipantau secara ketat.
- 13.2.8 Prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipelihara dan diterapkan pada implementasi sistem informasi.
- 13.2.9 Proses pengembangan dan integrasi sistem yang menjangkau seluruh siklus hidup pengembangan sistem harus diawasi dan dilindungi oleh Direktorat PTI.
- 13.2.10 Direktorat PTI harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan pihak ketiga atau vendor.
- 13.2.11 Pengujian fungsi keamanan harus dilakukan selama proses pengembangan baik sistem ataupun jaringan.

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : <b>16</b>

13.2.12 Program pengujian (*acceptance testing*) dan kriteria yang di *upgrade* atau versi terbaru harus ditetapkan untuk sistem informasi yang baru.

13.2.13 Data pengujian harus dipilih, dilindungi dan dikendalikan dengan teliti.

### 13.3 Dokumen Pendukung

- Tidak ada.

## 14. Pengendalian Pihak Ketiga (Vendor/Pemasok dan Provider/ Penyedia)

### 14.1 Tujuan

14.1.1 Memastikan aset-aset milik Universitas Bhayangkara Jakarta Raya yang dapat diakses oleh pihak ketiga aman dan terlindungi dari pihak yang tidak berwenang.

14.1.2 Mempertahankan tingkat keamanan informasi dan pelayanan yang telah disepakati dengan pihak ketiga.

### 14.2 Penerapan

14.2.1 Melakukan perjanjian kesepakatan dengan pemasok terhadap persyaratan keamanan Informasi Universitas Bhayangkara untuk mengurangi risiko terkait dengan akses pemasok ke dalam aset.

14.2.2 Semua persyaratan keamanan informasi yang sudah ditetapkan Universitas Bhayangkara Jakarta Raya harus disetujui oleh setiap pemasok yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur Teknologi Informasi.

14.2.3 Perjanjian kerjasama dengan pihak ketiga harus meliputi persyaratan untuk mengatasi risiko keamanan informasi yang terkait dengan teknologi informasi dan komunikasi layanan.

14.2.4 Universitas Bhayangkara Jakarta Raya harus secara berkala memonitor, mereview dan melakukan audit terhadap pelayanan dari pihak ketiga.

14.2.5 Perubahan dalam penyediaan layanan pihak ketiga harus dikelola dengan mempertimbangkan kekritisan dan penilaian risiko dari informasi, sistem, dan proses bisnis yang relevan.


### 14.3 Dokumen Pendukung

- Dokumen proses pengelolaan proyek (Prosedur, Instruksi Kerja, Standar, Aturan).
- *Non-Disclosure Agreement* (NDA) dengan Pihak Ketiga.
- Penilaian Layanan Pihak Ketiga.

## 15. Pengelolaan Insiden Keamanan Informasi

### 15.1 Tujuan

15.1.1 Memastikan pendekatan yang efektif dan konsisten terhadap pengelolaan insiden keamanan informasi dan mencakup komunikasi pada kejadian (*event*) dan

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : 17

kelemahan (*weakness*) terhadap keamanan Informasi.

- 15.1.2 Memastikan jika ada kejadian (*event*) kejadian dan kelemahan keamanan informasi yang berhubungan dengan sistem informasi dapat dikomunikasikan dan di ambil tindakan perbaikan yang tepat.

### 15.2 Penerapan

- 15.2.1 Prosedur pengelolaan insiden dan tanggung jawab harus ditetapkan dan diterapkan untuk memastikan respon yang cepat, efektif dan teratur terhadap insiden keamanan informasi.
- 15.2.2 Kejadian (*event*) keamanan informasi harus dilaporkan secepat mungkin sesuai prosedur dan mekanisme yang berlaku.
- 15.2.3 Karyawan dan PHL Universitas Bhayangkara Jakarta Raya yang menggunakan sistem dan layanan informasi harus mencatat dan melaporkan setiap kelemahan keamanan informasi dalam suatu sistem atau layanan.
- 15.2.4 Setiap kejadian (*event*) keamanan informasi harus dinilai, diputuskan dan diklasifikasikan sebagai insiden keamanan informasi.
- 15.2.5 Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur yang terdokumentasi
- 15.2.6 Pengetahuan yang diperoleh dari proses analisa dan penyelesaian masalah insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden di masa depan.
- 15.2.7 Universitas Bhayangkara Jakarta Raya harus menetapkan dan menerapkan mekanisme untuk mengidentifikasi, mengumpulkan, mengambil, dan menyimpan informasi pembuktian.

### 15.3 Dokumen Pendukung

- Manajemen Penanganan Insiden dan Permintaan *Support*.


## 16. Pengendalian Aspek Keamanan Informasi dalam Kestinambungan Usaha

### 16.1 Tujuan

- 16.1.1 Kestinambungan keamanan informasi harus tertanam dalam BCMS (*Business Continuity Management Systems*) pada Universitas.
- 16.1.2 Memastikan ketersediaan terhadap perangkat pengolahan informasi.

### 16.2 Penerapan

- 16.2.1 Universitas Bhayangkara Jakarta Raya harus menetapkan persyaratan untuk keamanan informasi dan kestinambungan terhadap pengelolaan keamanan informasi dalam situasi yang terburuk, misalnya selama krisis atau bencana.
- 16.2.2 Universitas Bhayangkara Jakarta Raya harus menetapkan, mendokumentasikan, menerapkan, dan memelihara proses, prosedur, dan kontrol untuk memastikan tingkat kestinambungan keamanan informasi yang diperlukan dalam keadaan yang merugikan.

	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : <b>18</b>

16.2.3 Universitas harus meninjau pelaksanaan dan menetapkan pengendalian terhadap kesinambungan keamanan informasi secara berkala sehingga proses tersebut valid dan efektif dalam situasi yang merugikan.

16.2.4 Fasilitas pengolahan informasi harus diterapkan untuk memenuhi persyaratan ketersediaan.

### 16.3 Dokumen Pendukung

- *Integrated Management System Plan (IMS Plan)*.
- Laporan uji coba *backup* dan *restore*.

## 17. Kepatuhan

### 17.1 Tujuan

17.1.1 Menghindari pelanggaran terhadap kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait dengan keamanan informasi dan persyaratan keamanan.

17.1.2 Memastikan bahwa keamanan informasi diimplementasikan dan diterapkan sesuai dengan peraturan Universitas Bhayangkara Jakarta Raya.

### 17.2 Penerapan

17.2.1 Seluruh undang-undang, peraturan, persyaratan kontrak dan pendekatan legislatif yang terkait serta pendekatan universitas untuk memenuhi persyaratan tersebut harus secara eksplisit diidentifikasi, didokumentasikan dan selalu *up-to-date*.

17.2.2 Semua undang-undang yang relevan, tata cara, persyaratan kontrak, pendekatan legislatif, dan pendekatan Universitas untuk memenuhi persyaratan ini diidentifikasi dengan jelas dan eksplisit, didokumentasikan, dan harus update untuk setiap sistem informasi.

17.2.3 Rekaman harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah dan rilis yang tidak sah, sesuai dengan legislasi, peraturan, persyaratan kontrak.

17.2.4 Perlindungan terhadap data dan informasi pribadi harus sesuai dengan undang-undang dan peraturan yang berlaku.

17.2.5 Kontrol terhadap kriptografi harus digunakan sesuai dengan semua perjanjian, undang-undang dan peraturan yang berlaku.

17.2.6 Pendekatan Universitas Bhayangkara Jakarta Raya dalam mengelola prosedur dan pelaksanaan keamanan informasi harus dikaji secara independen dan berkala ketika terjadi perubahan yang signifikan.


17.2.7 Direktur PTI harus secara teratur monitor kepatuhan terhadap proses pengolahan informasi dan prosedur dalam area tanggung jawab Direktur PTI, sesuai dengan kebijakan keamanan, standar dan persyaratan keamanan yang berlaku pada Universitas Bhayangkara Jakarta Raya.

17.2.8 Sistem informasi harus dikaji secara berkala untuk kepatuhan terhadap kebijakan dan standar keamanan informasi yang berlaku pada Universitas Bhayangkara Jakarta Raya.

### 17.3 Dokumen Pendukung

- Daftar peraturan perundang-undangan yang terkait keamanan informasi.



	<b>UNIVERSITAS BHAYANGKARA JAKARTA RAYA</b>	No : PTI/UBJ/CSIRT/001
		Tanggal : 24 Oktober 2023
	<b>KEBIJAKAN KEAMANAN INFORMASI (INFORMATION SECURITY POLICY)</b>	Revisi : -
		Halaman : <b>19</b>

- Laporan peninjauan kepatuhan terhadap keamanan informasi.

## 18. Kebijakan *Clear Desk - Clear Screen*

### 18.1 Tujuan

- 18.1.1 Melindungi informasi dan sistem informasi dari *human error* atau penyebaran secara tidak berwenang pada perangkat kerja.
- 18.1.2 Adanya panduan tata cara pengamanan informasi dan sistem informasi di Universitas Bhayangkara Jakarta Raya terutama di area kerja.
- 18.1.3 Mencegah dan mengendalikan risiko yang timbul karena kesalahan karyawan atau PHL dalam menggunakan perangkat pengolahan informasi.

### 18.2 Penerapan

- 18.2.1 Melindungi informasi dan sistem informasi dari *human error* atau penyebaran secara tidak berwenang pada perangkat kerja.
- 18.2.2 Saat menampilkan informasi sensitif di layar, karyawan harus waspada terhadap lingkungan sekitar mereka dan memastikan bahwa orang yang tidak berwenang tidak dapat melihat informasi yang ditampilkan.
- 18.2.3 Semua informasi yang menyangkut kesinambungan usaha yang bersifat rahasia atau kritis, seperti kertas atau *flashdisk/storage*, harus dilindungi, terutama saat karyawan meninggalkan tempat kerja.
- 18.2.4 Kertas yang mencantumkan informasi rahasia atau kritis harus segera diambil dari perangkat cetak.
- 18.2.5 Informasi rahasia atau penting yang terdapat pada kertas atau media penyimpanan elektronik harus segera dimusnahkan jika tidak digunakan atau disimpan di tempat yang aman sampai informasi tersebut dimusnahkan atau dihapus.

### 18.3 Dokumen Pendukung

- Tidak ada.