
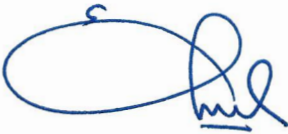




PT Infomedia Nusantara

***Statement of Applicability
(SOA)***

No. Dokumen	IN.DOK-01.02
Versi	1.0
Klasifikasi	Terbatas
Tanggal Efektif	08 September 2021
Tanggal Peninjauan	MALANG
Jenis Dokumentasi	Dokumen Acuan
Pemilik Dokumen	Koordinator Pengendali Dokumen

PERSETUJUAN:

DISUSUN:	MENGETAHUI:	DISETUJUI:
		
<u>Firdiansyah</u> Pengendali Dokumen	<u>Samudra Prasetio</u> Wakil Manajemen	<u>Agus Winarno</u> Manajemen Puncak

	<i>Statement of Applicability</i>	PT Infomedia Nusantara	
		No. Dokumen	IN.DOK-01.02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	1

RIWAYAT PERUBAHAN

Versi	Penyusun / Pelaksana Revisi	Tanggal Revisi	Keterangan Perubahan	Bab	Hal
1.0	Koordinator Pengendali Dokumen	08 September 2021	Versi pertama	-	-

infomedia CC TELKOM

CONTROLLED
DOCUMENT

MALANG

	Statement of Applicability	PT Infomedia Nusantara	
		No. Dokumen	IN.DOK-01.02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	1

Annex	Kontrol	Status Implementasi	Justifikasi	Referensi
A.5	Security Policy			
A.5.1	Management direction for information security			
A.5.1.1	Policies for information security	Ya		
A.5.1.2	Review of the policies for information security	Ya		
A.6	Organization of Information Security			
A.6.1	Internal Organization			
A.6.1.1	Information security roles and responsibility;	Ya		
A.6.1.2	Segregation of duties;	Ya		
A.6.1.3	Contact with authorities;	Ya		
A.6.1.4	Contact with special interest groups;	Ya		
A.6.1.5	Information security in project management	Ya		
A.6.2	Mobile devices and teleworking			
A.6.2.1	Mobile device policy;	Ya		
A.6.2.2	Teleworking.	Ya		
A.7	Human Resource Security			
A.7.1	Prior to Employment			
A.7.1.1	Screening;	Ya		

A.7.1.2	Terms and conditions of employment	Ya		
A.7.2	During employment			
A.7.2.1	Management responsibilities;	Ya		
A.7.2.2	Information security awareness, education and training;	Ya		
A.7.2.3	Disciplinary process.	Ya		
A.7.3	Termination or change of employment			
A.7.3.1	Termination or change of employment responsibilities	Ya		
A.8	Asset Management			
A.8.1	Responsibility for Assets			
A.8.1.1	Inventory of assets;	Ya		
A.8.1.2	Ownership of assets;	Ya		
A.8.1.3	Acceptable use of assets;	Ya		
A.8.1.4	Return of assets.	Ya		
A.8.2	Information classification			
A.8.2.1	Classification of information;	Ya		
A.8.2.2	Labelling of information;	Ya		
A.8.2.3	Handling of assets.	Ya		
A.8.3	Media Handling			
A.8.3.1	Management of removable media;	Ya		
A.8.3.2	Disposal of media;	Ya		
A.8.3.3	Physical media transfer	Ya		
A.9	Access Control			
A.9.1	Business requirement for access control			
A.9.1.1	Access control policy;	Ya		
A.9.1.2	Access to networks and network services	Ya		
A.9.2	User access management			
A.9.2.1	User registration and de-registration;	Ya		
A.9.2.2	User access provisioning;	Ya		

	<p style="text-align: center;">Statement of Applicability</p>	PT Infomedia Nusantara	
		No. Dokumen	IN.DOK-01.02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	3

A.9.2.3	Management of privileged access rights;	Ya		
A.9.2.4	Management of secret authentication information of users	Ya		
A.9.2.5	Review of user access rights;	Ya		
A.9.2.6	Removal or adjustment of access rights.	Ya		
A.9.3	User responsibilities			
A.9.3.1	Use of secret authentication information	Ya		
A.9.4	System and application access control			
A.9.4.1	Information access restriction;	Ya		
A.9.4.2	Secure log-on procedure;	Ya		
A.9.4.3	Password management system;	Ya		
A.9.4.4	Use of privileged utility programs;	Ya		
A.9.4.5	Access control to program source code.	Ya		
A.10	Cryptography			
A.10.1	Cryptographic controls			
A.10.1.1	Policy on the use of cryptographic controls;	Ya		
A.10.1.2	Key management	Ya		
A.11	Physical and Environmental Security			
A.11.1	Secure areas			
A.11.1.1	Physical security perimeter;	Ya		
A.11.1.2	Physical entry control;	Ya		

A.11.1.3	Securing offices, rooms and facilities;	Ya		
A.11.1.4	Protecting against external and environmental threats;	Ya		
A.11.1.5	Working in secure areas;	Ya		
A.11.1.6	Delivery and loading areas.	Ya		
A.11.2	Equipment			
A.11.2.1	Equipment siting and protection;	Ya		
A.11.2.2	Supporting utilities;	Ya		
A.11.2.3	Cabling security;	Ya		
A.11.2.4	Equipment maintenance;	Ya		
A.11.2.5	Removal of assets;	Ya		
A.11.2.6	Security of equipment and assets off-premises;	Ya		
A.11.2.7	Secure disposal or reuse of equipment;	Ya		
A.11.2.8	Unattended user equipment;	Ya		
A.11.2.9	Clear desk and clear screen policy.	Ya		
A.12	Operations Security			
A.12.1	Operational procedures and responsibilities			
A.12.1.1	Documented operation procedure;	Ya		
A.12.1.2	Change management;	Ya		
A.12.1.3	Capacity management;	Ya		
A.12.1.4	Separation of development, testing and operational environment.	Ya		
A.12.2	Protection from malware			
A.12.2.1	Control against malware	Ya		
A.12.3	Backup			
A.12.3.1	Information backup	Ya		
A.12.4	Logging and Monitoring			
A.12.4.1	Event logging;	Ya		
A.12.4.2	Protection of log information;	Ya		
A.12.4.3	Administrator and operator log;	Ya		

	Statement of Applicability	PT Infomedia Nusantara	
		No. Dokumen	IN.DOK-01.02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	5

A.12.4.4	Clock synchronization.	Ya		
A.12.5	Control of operational software			
A.12.5.1	Installation of software on operational systems	Ya		
A.12.6	Technical vulnerability management			
A.12.6.1	Management of technical vulnerabilities;	Ya		
A.12.6.2	Restrictions on software installation	Ya		
A.12.7	Information system audit considerations			
A.12.7.1	Information system audit control	Ya		
A.13	Communications Security			
A.13.1	Network security management			
A.13.1.1	Network controls;	Ya		
A.13.1.2	Security of network services;	Ya		
A.13.1.3	Segregation in networks	Ya		
A.13.2	Information transfer			
A.13.2.1	Information transfer policy and procedures;	Ya		
A.13.2.2	Agreements on information transfer;	Ya		
A.13.2.3	Electronic messaging;	Ya		
A.13.2.4	Confidentiality or non disclosure agreements	Ya		
A.14	System acquisition, development & maintenance			
A.14.1	Security requirements of information systems			

A.14.1.1	Information security requirements analysis and specification;	Ya		
A.14.1.2	Securing application services on public networks;	Ya		
A.14.1.3	Protecting application services transactions	Ya	CRM - On5, On4, Aplikasi CRM layanan, SSO - Newgen, SAP, e-recruitment, travel management	
A.14.2	Security in development and support processes			
A.14.2.1	Secure development policy;	Ya		
A.14.2.2	System change control procedure;	Ya		
A.14.2.3	Tech. review of applications after OS platform changes;	Ya		
A.14.2.4	Restrictions on changes to software packages;	Ya		
A.14.2.5	Secure system engineering principles;	Ya		
A.14.2.6	Secure development environment;	Ya		
A.14.2.7	Outsourced development;	No		
A.14.2.8	System security testing;	Ya		
A.14.2.9	System acceptances testing	Ya		
A.14.3	Test data			
A.14.3.1	Protection of test data	Ya		
A.15	Supplier relationship			
A.15.1	Information security in supplier relationship			
A.15.1.1	Information security policy for supplier relationship;	Ya		
A.15.1.2	Addressing security within supplier agreements;	Ya		
A.15.1.3	Information and communication technology supply chain.	Ya		
A.15.2	Supplier service delivery management			
A.15.2.1	Monitoring and review of supplier services;	Ya		
A.15.2.2	Managing changes to supplier services	Ya		
A.16	Information security incident management			
A.16.1	Management of information security incidents and improvements			

	<p style="text-align: center;">Statement of Applicability</p>	PT Infomedia Nusantara	
		No. Dokumen	IN.DOK-01.02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	7

A.16.1.1	Responsibilities and procedures;	Ya		
A.16.1.2	Reporting informations security events;	Ya		
A.16.1.3	Reporting informations security weaknesses;	Ya		
A.16.1.4	Assessment of and decision on information security events;	Ya		
A.16.1.5	Response to information security incidents;	Ya		
A.16.1.6	Learning from information security incidents;	Ya		
A.16.1.7	Collection of evidence	Ya		
A.17	Information security aspects of business continuity management			
A.17.1	Information security continuity			
A.17.1.1	Planning information security continuity;	Ya		
A.17.1.2	Implementing informations security continuity;	Ya		
A.17.1.3	Verify, review and evaluate Information Security continuity	Ya		
A.17.2	Redundancies			
A.17.2.1	Availability of information processing facilities	Ya		
A.18	Compliance			
A.18.1	Compliance with legal and contractual requirements			
A.18.1.1	Identification of applicable legislation & contractual requirements;	Ya		

A.18.1.2	Intellectual property rights;	Ya		
A.18.1.3	Protection of records;	Ya		
A.18.1.4	Privacy & protection of personally identifiable information.	Ya		
A.18.1.5	Regulation of cryptographic controls	Ya		
A.18.2	Information security reviews			
A.18.2.1	Independent review of information security;	Ya		
A.18.2.2	Compliance with security policies and standard;	Ya		
A.18.2.3	Technical compliance review	Ya		

KETERANGAN:

Jumlah kontrol yang tidak diimplementasikan: 1 kontrol

Jumlah kontrol yang diimplementasikan: 0 kontrol