

## DAFTAR ISI

LEMBAR PENGESAHAN.....	ii
ABSTRAK .....	iii
<i>ABSTRACT</i> .....	iv
LEMBAR PERSEMBAHAN.....	v
KATA PENGANTAR .....	vii
LEMBAR PERNYATAAN ORISINALITAS.....	viii
DAFTAR ISI .....	ix
DAFTAR GAMBAR .....	xiii
DAFTAR TABEL .....	xvi
DAFTAR LAMPIRAN.....	xviii
DAFTAR ISTILAH.....	xix
DAFTAR SINGKATAN .....	xx
BAB I PENDAHULUAN .....	1
I.1    Latar Belakang.....	1
I.2    Perumusan Masalah .....	5
I.3    Tujuan Penelitian.....	6
I.4    Batasan Penelitian.....	6
I.5    Manfaat Penelitian .....	6
I.5.1    Manfaat Teoritis .....	6
I.5.2    Manfaat Praktis.....	6
I.6    Sistematika Penulisan .....	7
BAB II LANDASAN TEORI .....	9
II. 1 <i>Interconnection Network</i> (Internet) .....	9
II. 2    Jaringan Komputer.....	9
II.2.1 <i>Local Area Network</i> (LAN).....	10
II.2.2 <i>Wide Area Netwrok</i> (WAN).....	10

II. 3	Keamanan Komputer .....	10
II. 4	Keamanan Jaringan Komputer .....	11
II. 5	<i>Firewall</i> .....	11
II. 6	<i>Proxy Server</i> .....	12
II. 7	<i>Intrusion Detection System (IDS)</i> .....	13
II. 8	<i>Virtual Local Area Network (VLAN)</i> .....	13
II. 9	<i>Virtual Private Network (VPN)</i> .....	14
II. 10	<i>Access Control List (ACL)</i> .....	15
II. 11	<i>Network Development Life Cycle (NDLC)</i> .....	16
II.11.1	<i>Analysis</i> .....	17
II.11.2	<i>Design</i> .....	18
II.11.3	<i>Simulation Prototyping</i> .....	18
II.11.4	<i>Implementation</i> .....	18
II.11.5	<i>Monitoring</i> .....	18
II.11.6	<i>Management</i> .....	18
II. 12	<i>Information Security Management System (ISMS)</i> .....	19
II. 13	ISO/IEC 27000.....	19
II.13.1	ISO/IEC 27001.....	20
II.13.2	ISO/IEC 27002.....	20
II. 14	Penelitian Sebelumnya .....	21
<b>BAB III METODOLOGI PENELITIAN</b> .....		23
III.1	Metode Konseptual .....	23
III.2	Sistematika Pemecahan Masalah .....	25
III.2.1	Tahap Awal .....	27
III.2.2	Tahap Analisis .....	27
III.2.3	Tahap Desain .....	27

III.2.4	Tahap Simulasi .....	27
III.2.5	Tahap Akhir.....	28
BAB IV	ANALISIS KONDISI SAAT INI.....	29
IV.1	Profil Lembaga.....	29
IV.1.1	Visi Yakes Telkom .....	30
IV.1.2	Misi Yakes Telkom.....	30
IV.1.3	Struktur Organisasi .....	32
IV.1.4	Rencana Jangka Panjang (RJP) Yakes Telkom 2016-2020.....	34
IV.1.5	<i>Value Chain</i> Yayasan Kesehatan (Yakes) Telkom.....	35
IV.2	Kondisi Jaringan Saat Ini.....	36
IV.2.1	Topologi Fisik Jaringan Saat Ini.....	36
IV.2.2	Topologi Logik Jaringan Saat Ini .....	40
IV.2.3	Spesifikasi Aplikasi Yakes Telkom.....	43
IV.2.4	Aliran Data Aplikasi .....	48
IV.2.5	Kondisi Keamanan Jaringan Saat Ini.....	49
IV.2.6	Perangkat Jaringan Fisik Saat Ini .....	53
IV.2.7	Kebijakan dan Kontrol Keamanan Jaringan Saat Ini.....	60
IV.2.8	Celah Keamanan <i>Server</i> .....	65
IV.2.9	<i>Monitoring</i> dan <i>Helpdesk</i> .....	68
IV.2.10	Sumber Daya Manusia Bidang Teknologi .....	74
IV.3	Insiden Keamanan Jaringan pada Yakes Telkom <i>Open Access</i> .....	75
IV.4	Dampak Yang Ditimbulkan dari Insiden Keamanan <i>Open Access</i> .....	76
BAB V	ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN USULAN.....	78
V.1	Desain Keamanan Jaringan Komputer Usulan.....	78
V.1.1	Penerapan <i>Firewall</i> .....	80
V.1.2	<i>Logging and Monitoring System</i> .....	82

V.1.3	Optimasi <i>Web Protection</i> untuk Mencegah <i>Open Access</i> Menggunakan <i>Proxy Server</i> .....	85
V.1.4	Optimasi <i>Open Port Server</i> .....	87
V.2	Skenario Pengujian Keamanan Usulan .....	89
V.2.1	Topologi Pengujian.....	90
V.2.2	Pengujian Penerapan <i>Firewall</i> sebagai DMZ.....	91
V.2.3	Pengujian Optimasi <i>Web Protection</i> .....	95
V.3	Perancangan Kontrol Keamanan Usulan .....	99
BAB VI KESIMPULAN DAN SARAN .....		101
VI.1	Kesimpulan .....	101
VI.2	Saran.....	102
DAFTAR PUSTAKA .....		103