DAFTAR ISI

ABSTRAK v
ABSTRACT iv
KATA PENGANTAR iiv
DAFTAR ISI v
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR SIMBOL xiv
DAFTAR LAMPIRAN xv
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Identifikasi Masalah 2
1.3 Maksud dan Tujuan 2
1.3.1 Maksud 2
1.3.2 Tujuan 3
1.4 Batasan Masalah 3
1.5 Metodologi Penelitian 3
1.6 Sistematika Penulisan 5
BAB II TINJAUAN PUSTAKA 7
2.1 Profil Perusahaan 7
2.1.1 Sejarah Perusahaan 7
2.1.2 Visi Perusahaan 7
2.1.3 Misi Perusahaan 8
2.1.4 Struktur Organisasi 8
2.1.5 Job Description 10
2.1.5.1 Job Description Bidang Program 10
2.1.5.2 Job Descripton Bidang Berita 10
2.1.5.3 Job Description Bidang Teknik 10
2.2 Landasan Teori 10
2.2.1 Jaringan 10
2.2.1.1 Jaringan Komputer 11

2.2.1.2 Jenis-Jenis Koneksi 11
2.2.1.3 Topologi Fisik 12
2.2.1.4 Kategori Jaringan Komputer 12
2.2.2 Risiko 14
2.2.1.5 Manajemen Risiko 14
2.2.1.6 Pengukuran Risiko 14
2.2.1.7 Analisis Risiko 16
2.2.1.8 Penanganan Risiko 16
2.2.3 Aset 17
2.2.2.1 Informasi Aset 17
2.2.2.2 Identifikasi Aset 18
2.2.2.3 Manajemen Aset 18
2.2.2.2 Analisis Aset 19
2.2.2.3 Analisis Kerentanan Aset 19
2.2.5 Keamanan 20
2.2.3.1 Keamanan Jaringan Komputer 20
2.2.3.2 Keamanan Informasi 21
2.2.6 ISO 21
2.2.6.1 SNI ISO/IEC 27001 22
2.2.6.2 Manfaat menerapkan SNI ISO/IEC 27001 22
2.2.6.3 Parameter SNI ISO/IEC 27001 23
2.2.7 Nmap 49
2.2.8 Nessus 49
BAB III ANALISIS DAN PERANCANGAN SISTEM 51
3.1 Ruang Lingkup Keamanan Informasi 51
3.1.1 Analisis Masalah 51
3.1.2 Analisis Kondisi Eksisting 51
3.1.2.1 Analisis Denah Ruangan 52
3.1.2.2 Analisis Jaringan Komputer 55
3.1.2.3 Analisis Konfigurasi Pengalamatan IP 56
3.1.3 Analisis Parameter SNI ISO/IEC 27001 57

3.2 A.8 Manajemen Aset 93
3.2.1 A.8.1.1 Inventaris Aset 93
3.2.2 A.8.1.2 Kepemilikan Aset 94
3.2.3 A.8.1.3 Penggunaan Yang Dapat Diterima Atas Aset 95
3.2.4 A.8.1.4 Pengembalian Aset 96
3.3 A.9 Kendali Akses 96
3.3.1 A.9.1.2 Akses Ke Jaringan dan Layanan Jaringan 96
3.3.2 A.9.2.2 Penyediaan Akses Pengguna 97
3.3.3 A.9.4.1 Pembatasan Akses Informasi 97
3.4 A.11 Keamanan Fisik dan Lingkungan 97
3.4.1 A.11.1.1 Batas Fisik keamanan 97
3.4.2 A.11.1.2 Kendali Masuk Fisik 100
3.4.3 A.11.2.1 Penempatan dan Perlindungan Peralatan 100
3.4.4 A.11.2.3 Keamanan Kabel 101
3.4.5 A.11.2.4 Pemeliharaan Peralatan 101
3.5 A.12 Keamanan Operasi 102
3.5.1 A.12.2.1 Kendali Terhadap Malware 102
3.5.2 A.12.3.1 Cadangan Informasi 103
3.5.3 A.12.4.1 Pencatatan Kejadian 103
3.5.4 A.12.4.2 Perlindungan Terhadap Informasi Log 104
3.5.5 A.12.6.1 Manajemen Kerentanan Teknis 104
3.6 A.13 Keamanan Komunikasi 104
3.6.1 A.13.1.1 Kendali Jaringan 104
3.6.2 A.13.1.2 Keamanan Layanan Jaringan 105
3.6.3 A.13.1.3 Pemisahan Dalam Jaringan 114
3.7 Manajemen Risiko 117
3.7.1 Risiko Manajemen Aset 117
3.7.1.1 Risiko Terhadap Inventaris Aset 117
3.7.1.2 Risiko Terhadap Kepemilikan Aset 119
3.7.2 Risiko Kendali Akses 120
3.7.2.1 Risiko Akses ke Jaringan dan Layanan Jaringan 120

3.7.2.2 Risiko Penyediaan Akses Pengguna 120
3.7.3 Risko Keamanan Fisik dan Lingkungan 121
3.7.3.1 Batas Fisik Keamanan 121
3.7.3.2 Kendali Masuk Fisik 121
3.7.3.3 Penyimpanan dan Perlindungan Peralatan 122
3.7.3.4 Keamanan Kabel 122
3.7.3.5 Pemeliharaan Peralatan 123
3.7.4 Risiko Keamanan Operasi 124
3.7.4.1 Kendali Terhadap Malware 124
3.7.4.2 Cadangan Inforamsi 125
3.7.4.3 Pencatatan Kejadian 125
3.7.5 Risiko Keamanan Komunikasi 126
3.7.5.1 Kendali Jaringan 126
3.7.5.2 Pemisahan Dalam Jaringan 127
BAB III PENGUJIAN 129
4.1 Pengujian Manajemen Aset 129
4.1.1 Pengujian Inventaris Aset 129
4.1.1.1 Analisis dan Rekomendasi 129
4.1.2 Pengujian Kepemilikan Aset 130
4.1.2.1 Analisis dan Rekomendasi 130
4.1.3 Pengujian Penggunaan Yang Dapat Diterima 130
4.1.3.1 Analisis dan Rekomendasi 131
4.1.4 Pengujian Pengembalian Aset 131
4.1.4.1 Analisis dan Rekomendasi 132
4.2 Pengujian Kendali Akses 132
4.2.1 Pengujian Akses Ke Jaringan dan Layanan 132
4.2.1.1 Analisis dan Rekomendasi 133
4.2.2 Pengujian Penyediaan Akses Pengguna 133
4.2.2.1 Analisis dan Rekomendasi 134
4.2.3 Pengujian Pembatasan Akses Informasi 134
4.2.3.1 Analisis dan Rekomendasi 135

4.3 Pengujian Keamanan Fisik dan Lingkungan 135
4.3.1 Pengujian Batas Fisik Keamanan 135
4.3.1.1 Analisis dan Rekomendasi 136
4.3.2 Pengujian Penempatan dan Perlindungan Peralatan 136
4.3.2.1 Analisis dan Rekomendasi 137
4.3.3 Pengujian Keamanan Kabel 137
4.3.3.1 Analisis dan Rekomendasi 138
4.3.4 Pengujian Pemeliharaan Peralatan 138
4.3.4.1 Analisis dan Rekomendasi 139
4.4 Pengujian Keamanan Operasi 139
4.4.1 Pengujian Kendali Terhadap Malware 139
4.4.1.1 Analisis dan Rekomendasi 139
4.4.2 Pengujian Cadangan Informasi 140
4.4.2.1 Analisis dan Rekomendasi 140
4.4.3 Pengujian Pencatatan Kejadian 140
4.4.3.1 Analisis dan Rekomendasi 141
4.4.4 Pengujian Perlindungan Terhadap Informasi Log 141
4.4.4.1 Analisis dan Rekomendasi 141
4.4.5 Pengujian Manajemen Kerentanan Teknis 142
4.4.5.1 Analisis dan Rekomendasi 142
4.5 Pengujian Keamanan Komunikasi 142
4.5.1 Pengujian Kendali Jaringan 142
4.5.1.1 Analisis dan Rekomendasi 143
4.5.2 Pengujian Keamanan Layanan Jaringan 143
4.5.2.1 Analisis dan Rekomendasi 146
4.5.3 Pengujian Pemisahan Dalam Jaringan 147
4.5.3.1 Analisis dan Rekomendasi 147
4.6 Pengujian Aspek SNI ISO/IEC 27001 147
4.7 Roadmap SMKI (Sistem Manajemen Keamanan Informais) 153
4.8 Kesimpulan Hasil Pengujian 162
BAB V 163

5.1 Kesimpulan 163
5.2 Saran 163
DAFTAR PUSTAKA 164