

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

Sommaire général des services de sécurité

Introduction	3
Sommaire général des services de sécurité	7
Domaine 1 : Organisation	15
01A Rôles et structures de la sécurité	15
01A01 Organisation du management et du pilotage de la sécurité générale	17
01A02 Organisation du management et du pilotage de la sécurité des SI	18
01A03 Système général de reporting et de gestion des incidents	19
01A04 Organisation des audits et du plan d'audit	20
01A05 Gestion de crise liée à la sécurité de l'information	21
01B Référentiel de sécurité	22
01B01 Devoirs et responsabilités du personnel et du management	22
01B02 Directives générales de protection de l'information	23
01B03 Classification des ressources	24
01B04 Gestion des actifs	25
01C Gestion des ressources humaines	26
01C01 Engagements du personnel – clauses contractuelles	26
01C02 Gestion du personnel stratégique	27
01C03 Procédures d'habilitation du personnel	28
01C04 Sensibilisation et formation du personnel	29
01C05 Gestion des tierces parties	30
01C06 Enregistrement des personnes	31
01D Assurances	32
01D01 Assurance des dommages matériels	32
01D02 Assurance des dommages immatériels	33
01D03 Assurance Responsabilité Civile	34
01D04 Assurance Perte de Personnages clés	35
01E Continuité de l'activité	36
01E01 Prise en compte des besoins de continuité de l'activité	36
01E02 Plans de Continuité de l'activité	37
Domaine 2 : Sécurité des sites et bâtiments	38
02A Contrôle d'accès physique au site et aux bâtiments	38
02A01 Gestion des droits d'accès au site ou à l'immeuble	39
02A02 Gestion des autorisations d'accès au site ou à l'immeuble	40
02A03 Contrôle d'accès au site ou à l'immeuble	41
02A04 Détection des intrusions sur le site ou dans l'immeuble	42

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

02A05	Accès aux zones de déchargement ou de chargement	43
Domaine 3 : Sécurité des locaux		44
03A	Services généraux	46
03A01	Qualité de la fourniture de l'énergie	46
03A02	Continuité de la fourniture de l'énergie	47
03A03	Sécurité de la climatisation	48
03A04	Qualité du câblage	49
03A05	Protection contre la foudre	50
03B	Contrôle d'accès aux locaux sensibles	51
03B01	Gestion des droits d'accès aux locaux sensibles	51
03B02	Gestion des autorisations d'accès aux locaux sensibles	52
03B03	Contrôle d'accès aux locaux sensibles	53
03B04	Détection des intrusions dans les locaux sensibles	54
03B05	Surveillance périmétrique des locaux sensibles	55
03B06	Surveillance des locaux sensibles	56
03B07	Contrôle d'accès au câblage	57
03B08	Localisation des locaux sensibles	58
03C	Sécurité contre les dégâts des eaux	59
03C01	Prévention des risques de dégâts des eaux	59
03C02	Détection des dégâts des eaux	60
03C03	Évacuation de l'eau	61
03D	Sécurité contre l'incendie	62
03D01	Prévention des risques d'incendie	62
03D02	Détection incendie	63
03D03	Extinction incendie	64
03E	Protection contre les risques environnementaux divers	65
03E01	Protection contre les risques environnementaux divers	65
Domaine 4 : Réseau étendu intersites		66
04A	Sécurité de l'architecture du réseau étendu et continuité de service	68
04A01	Sûreté de fonctionnement des éléments d'architecture du réseau étendu	68
04A02	Télépilotage de l'exploitation du réseau étendu	69
04A03	Organisation de la maintenance des équipements du réseau étendu	70
04A04	Procédures et plans de reprise du réseau étendu sur incidents	71
04A05	Plan de sauvegarde des configurations du réseau étendu	72
04A06	Plan de sauvegarde des données applicatives du réseau étendu	73
04A07	Plan de Reprise d'Activité (PRA) du réseau étendu	74
04B	Contrôle des connexions sur le réseau étendu	76
04B01	Profils de sécurité des entités connectées au réseau étendu	76

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

04B02	Authentification de l'entité accédante lors d'accès entrants depuis le réseau étendu	77
04B03	Authentification de l'entité accédée, lors d'accès sortants vers d'autres entités par le réseau étendu	78
04C	Sécurité des données lors des échanges et des communications	79
04C01	Chiffrement des échanges sur le réseau étendu	79
04C02	Contrôle de l'intégrité des échanges sur le réseau étendu	80
04D	Détection et traitement des incidents sur le réseau étendu	81
04D01	Surveillance en temps réel du réseau étendu	81
04D02	Surveillance en temps différé des traces, logs et journaux d'événements sur le réseau étendu	82
04D03	Traitement des incidents du réseau étendu	83
Domaine 5 : Réseau local.....		84
05A	Sécurité de l'architecture du réseau local	86
05A01	Partitionnement du réseau local en domaines de sécurité	86
05A02	Sûreté de fonctionnement des éléments d'architecture du réseau local	87
05A03	Télépilote de l'exploitation du réseau local	88
05A04	Organisation de la maintenance des équipements du réseau local	89
05A05	Procédures et plans de reprise du réseau local sur incidents	90
05A06	Plan de sauvegarde des configurations du réseau local	91
05A07	Plan de sauvegarde des données applicatives du réseau local	92
05A08	Plan de Reprise d'Activité (PRA) du réseau local	93
05A09	Gestion des fournisseurs critiques du réseau local (vis-à-vis de la permanence de la maintenance)	94
05B	Contrôle d'accès au réseau local de données	95
05B01	Gestion des profils d'accès au réseau local de données	95
05B02	Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)	96
05B03/05B05/05B06	Authentification de l'accédant lors de l'accès au réseau local	97
05B04	Authentification de l'accédant lors de l'accès au réseau local depuis un site distant via le réseau étendu	99
05B07	Filtrage général des accès au réseau local	100
05B08	Contrôle du routage des accès sortants	101
05B09	Authentification de l'entité accédée, lors d'accès sortants vers des sites sensibles	102
05C	Sécurité des données lors des échanges et des communications sur le réseau local ...	103
05C01	Chiffrement des échanges sur le réseau local	103
05C03	Chiffrement des échanges lors des accès distants au réseau local	103
05C02	Protection de l'intégrité des échanges sur le réseau local	104
05C04	Protection de l'intégrité des échanges lors des accès distants au réseau local	104
05D	Détection et traitement des incidents et anomalies du réseau local	105
05D01	Surveillance en temps réel du réseau local	105

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

05D02	Surveillance en temps différé des traces, logs et journaux des événements sur le réseau local	106
-------	---	-----

05D03	Traitement des incidents du réseau local	107
-------	--	-----

Domaine 6 : Exploitation des réseaux 108

06A	Sécurité des procédures d'exploitation.....	110
------------	--	------------

06A01	Prise en compte de la sécurité dans les relations avec le personnel d'exploitation.....	110
-------	---	-----

06A02	Contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels.....	111
-------	---	-----

06A03	Contrôles des opérations de maintenance	112
-------	---	-----

06A04	Contrôle de la télémaintenance	113
-------	--------------------------------------	-----

06A05	Gestion des procédures opérationnelles	114
-------	--	-----

06A06	Gestion des prestataires de service	115
-------	---	-----

06A07	Prise en compte de la confidentialité lors des opérations de maintenance sur les équipements de réseau	116
-------	--	-----

06A08	Gestion des contrats de services réseaux.....	117
-------	---	-----

06B	Paramétrage et contrôle des configurations matérielles et logicielles.....	118
------------	---	------------

06B01	Paramétrage des équipements de réseau et contrôle des configurations	118
-------	--	-----

06B02	Contrôle des configurations Utilisateurs	119
-------	--	-----

06C	Contrôle des droits d'administration	120
------------	---	------------

06C01	Gestion des droits privilégiés sur les équipements de réseau	120
-------	--	-----

06C02	Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation	121
-------	--	-----

06C03	Surveillance des actions d'administration des réseaux	122
-------	---	-----

06C04	Contrôle des outils et utilitaires de l'exploitation	123
-------	--	-----

06D	Procédures d'audit et de contrôle des réseaux.....	124
------------	---	------------

06D01	Fonctionnement des contrôles d'audit.....	124
-------	---	-----

06D02	Protection des outils et résultats d'audit	125
-------	--	-----

Domaine 7 : Sécurité des systèmes et de leur architecture..... 126

07A	Contrôle d'accès aux systèmes et applications.....	128
------------	---	------------

07A1	Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction)	128
------	---	-----

07A2	Gestion des autorisations d'accès et privilèges (attribution, délégation, retrait)	129
------	--	-----

07A3	Authentification de l'accédant	130
------	--------------------------------------	-----

07A4	Filtrage des accès et gestion des associations	131
------	--	-----

07B	Confinement des environnements	132
------------	---	------------

07B1	Contrôle des accès aux résidus.....	132
------	-------------------------------------	-----

07C	Gestion et enregistrement des traces.....	133
------------	--	------------

07C1	Enregistrement des accès aux ressources sensibles.....	133
------	--	-----

07C2	Enregistrement des appels aux procédures privilégiées	134
------	---	-----

07D	Sécurité de l'architecture	135
------------	---	------------

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

07D1	Sûreté de fonctionnement des éléments d'architecture	135
07D02	Isolement des systèmes sensibles	136
Domaine 8 : Production informatique		137
08A	Sécurité des procédures d'exploitation	140
08A01	Prise en compte de la sécurité de l'information dans les relations avec le personnel d'exploitation	140
08A02	Contrôle des outils et utilitaires de l'exploitation	141
08A03	Télépilotage de l'exploitation	142
08A04	Contrôle de la mise en production de nouveaux systèmes ou d'évolutions de systèmes existants	143
08A05	Contrôle des opérations de maintenance	144
08A06	Prise en compte de la confidentialité lors des opérations de maintenance (matérielle et logicielle) sur des systèmes de production	145
08A07	Contrôle de la télémaintenance	146
08A08	Diffusion des états imprimés sensibles	147
08A09	Gestion des procédures opérationnelles	148
08A10	Gestion des prestataires de service	149
08B	Paramétrage et contrôle des configurations	150
08B01	Paramétrage des systèmes et contrôle des configurations systèmes	150
08B02	Contrôle des configurations applicatives	150
08B03	Contrôle de la conformité des programmes de référence	151
08B04	Contrôle des configurations Utilisateurs	152
08B05	Contrôle du caractère licite des licences logicielles	153
08C	Gestion des supports informatiques de données et programmes	154
08C01	Administration des supports	154
08C02	Marquage des supports de production	155
08C03	Sécurité physique des supports de production stockés sur site	156
08C04	Sécurité physique des supports externalisés (stockés sur site externe)	157
08C05	Vérification et rotation des supports d'archivage	158
08C06	Protection des réseaux de stockage (SAN : Storage Area Network)	159
08D	Continuité de fonctionnement	161
08D01	Organisation de la maintenance du matériel	161
08D02	Organisation de la maintenance du logiciel	162
08D03	Procédures et plans de reprise des applications sur incidents	163
08D04	Sauvegarde des logiciels de base et applicatifs	164
08D05	Sauvegarde des données applicatives	165
08D06	Plans de reprise d'activité	166
08D07	Protection antivirale des serveurs de production	167
08D08	Gestion des systèmes critiques (vis-à-vis de la permanence de la maintenance)	168
08D09	Sauvegarde de recours externalisées	169

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

08E	Détection et traitement des incidents et anomalies.....	170
08E01	Détection et traitement en temps réel des anomalies et incidents.....	170
08E02	Surveillance en temps différé des traces, logs et journaux.....	171
08E03	Gestion et traitement des incidents systèmes et applicatifs.....	172
08F	Contrôle des droits d'administration	173
08F01	Gestion des droits privilégiés sur les systèmes.....	173
08F02	Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation	174
08F03	Surveillance des actions d'administration des systèmes.....	175
08G	Procédures d'audit et de contrôle des systèmes de traitement de l'information.....	176
08G01	Fonctionnement des contrôles d'audit.....	176
08G02	Protection des outils et résultats d'audit	177
Domaine 9 : Sécurité applicative		178
09A	Contrôle d'accès applicatif	181
09A01	Gestion des profils d'accès aux données applicatives	181
09A02	Gestion des autorisations d'accès aux données applicatives	182
09A03	Authentification lors de l'accès aux données applicatives.....	183
09A04	Filtrage des accès aux données applicatives	184
09B	Contrôle de l'intégrité des données	185
09B01	Scellement des données sensibles (fichiers)	185
09B02	Protection de l'intégrité des données échangées	186
09B03	Contrôle de la saisie des données.....	187
09B04	Contrôles permanents.....	188
09C	Contrôle de la confidentialité des données.....	189
09C01	Chiffrement des données échangées	189
09C02	Chiffrement des données stockées	190
09C03	Dispositif anti-rayonnement	191
09D	Disponibilité des données	192
09D01	Enregistrement de Très Haute Sécurité (THS).....	192
09D02	Reconstitution des données	193
09D03	Reconstitution des traitements	194
09D04	Organisation de l'archivage	195
09E	Continuité de fonctionnement.....	196
09E01	Reconfiguration matérielle	196
09E02	Plans de Continuité Utilisateurs.....	197
09E03	Plans d'urgence	198
09E04	Gestion des applications critiques (vis-à-vis de la permanence de la maintenance).....	199
09E05	Reconstitution des programmes de traitement.....	200
09F	Contrôle de l'émission et de la réception des données	201

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

09F01	Garantie d'origine – signature électronique	201
09F02	Individualisation des messages empêchant leur duplication.....	202
09F03	Accusé de réception	203
09G	Détection et gestion des incidents et anomalies applicatifs	204
09G01	Détection et traitement des incidents et anomalies applicatifs	204
09H	Services et applications liés au commerce électronique.....	205
09H01	Sécurité des sites de commerce électronique	205
Domaine 10	: Sécurité des projets et développements applicatifs	206
10A	Organisation interne des développements et de la maintenance	207
10A01	Prise en compte de la sécurité dans les projets et développements	207
10A02	Gestion des changements	208
10A03	Externalisation du développement logiciel	209
10A04	Organisation de la maintenance applicative	210
10A05	Modification des progiciels.....	211
10B	Sécurité des processus des développements et de la maintenance.....	212
10B01	Sécurité des processus des développements applicatifs	212
10B02	Protection de la confidentialité des développements applicatifs	213
10B03	Sécurité relative aux traitements internes des applications	214
10B04	Protection des données d'essai	215
10B06	Maintenance à chaud	217
Domaine 11	: Protection de l'environnement de travail	218
11A	Contrôle des accès aux zones de bureaux	220
11A01	Partitionnement des bureaux en domaines de sécurité et cloisonnement.....	220
11A02	Gestion des autorisations aux zones de bureaux protégées	221
11A03	Détection des intrusions dans les zones de bureaux protégées	222
11A04	Surveillance des zones de bureaux protégées.....	223
11A05	Contrôle de la circulation des visiteurs et prestataires occasionnels	224
11B	Protection de l'information écrite	225
11B01	Conservation et protection des pièces originales et éléments de preuve ou considérées comme des valeurs patrimoniales	225
11B02	Rangement des bureaux et protection des documents et supports sensibles	226
11B03	Ramassage des corbeilles à papier et destruction des documents	227
11B04	Sécurité du courrier.....	228
11B05	Sécurité des fax	229
11B06	Sécurité des autocommutateurs	230
11B07	Sécurité de la messagerie électronique et des échanges électroniques d'information.....	231
11C	Protection des postes de travail	232
11C01	Contrôle d'accès au poste de travail.....	232
11C02	Protection de la confidentialité des données stockées sur le poste de travail	233

CLUSIF Espace Méthodes	MEHARI Manuel de référence des Services de sécurité	Version 2007 23 février 2007
---------------------------	--	---------------------------------

11C03	Prise en compte de la confidentialité lors des opérations de maintenance des postes utilisateurs	234
11C04	Protection de l'intégrité des données stockées sur le poste de travail	235
11C05	Travail en dehors des locaux de l'entreprise	236
11C06	Utilisation d'équipements personnels	237
11D	Continuité de service de l'environnement de travail	238
11D01	Organisation de la maintenance du matériel mis à la disposition du personnel	238
11D02	Organisation de la maintenance du logiciel des postes utilisateurs	239
11D03	Plans de sauvegardes des configurations utilisateurs	240
11D04	Plan de sauvegarde des données utilisateurs stockées sur serveur	241
11D05	Plan de sauvegarde des données utilisateurs stockées sur le poste	242
11D06	Plans de protection antivirale des postes de travail	243
11D07	Plan de Reprise de l'Environnement de Travail	244
Domaine 12 : Domaine juridique et réglementaire		245
12A	Respect de la réglementation concernant les rapports avec le personnel ou des tiers ..	245
12B	Protection de la propriété intellectuelle	245
12D	Respect de la réglementation extérieure et de la législation concernant la cryptologie ..	245
12A01	Respect de la réglementation extérieure et de la législation concernant le respect de la vie privée	247
12A02	Respect de la réglementation extérieure et de la législation concernant les accès non autorisés à des systèmes tiers	247
12B01	Respect de la réglementation extérieure et de la législation concernant la protection de la propriété des logiciels	247
12D01	Respect de la réglementation extérieure et de la législation concernant l'usage de la cryptologie	247
12C	Respect de la législation concernant la communication financière	248
12C01	Respect de la réglementation extérieure et de la législation concernant la communication financière	248
12E	Respect de la réglementation concernant la vérification de la comptabilité informatisée ..	249
12E01	Conservation des données et traitements	249
12E02	Documentation des données, procédures et traitements liés à la comptabilité	250