RSSI-CNRS

N° règle	Chapitre	Sensibilité	Règle	N° ISO	Chapitre ISO	Mesures ISO
POL-1	Politique	*	Les règles de la PSSI opérationnelle de l'unité sont définies après détermination du niveau de couverture des risques applicable.	5	Politique de sécurité	5.1.1, 8.2.2
ORG-1	Organisation	*	Le DU est responsable de la sécurité des systèmes d'information (SSI) dans son unité et nomme une personne chargée de la SSI (CSSI) pour l'assister en la matière	6	Organisation de la sécurité de l'information	6.1.1, 6.1.2, 6.1.3
ORG-2	Organisation	*	Le DU est responsable de la formalisation et du suivi du plan d'action de mise en œuvre des règles de la PSSI dans l'unité	6	Organisation de la sécurité de l'information	6.1.1
ORG-3	Organisation	*	La sensibilisation à la SSI de l'ensemble des personnels de l'unité doit être réalisée	6	Organisation de la sécurité de l'information	8.2.2
ORG-5	Organisation	*	La SSI doit être prise en compte dans les contrats avec les tiers.	6	Organisation de la sécurité de l'information	6.2.3
ORG-6	Organisation	*	Toute dérogation aux règles de cette PSSI doit être validée par le DU avec avis motivé	6	Organisation de la sécurité de l'information	27001 4.2.1j
ORG-7	Organisation	***	Le DU, en collaboration avec le CSSI, RSI et tout autre acteur impliqué dans la démarche sécurité, définit et formalise les responsabilités de chacun concernant les mesures SSI à mettre en œuvre.	6	Organisation de la sécurité de l'information	6.1.3
PDI-1	Protection des documents et des informations	*	Les documents électroniques produits dans l'unité doivent être marqués par leur producteur suivant leur niveau de confidentialité : diffusion publique, diffusion interne, diffusion restreinte.	7	Gestion des actifs	7.2.1
PDI-2	Protection des documents et des informations	*	Les documents électroniques doivent être stockés, manipulés, transmis via les procédures et avec les outils propres à assurer leur confidentialité au niveau adéquat.	7	Gestion des actifs	7.2.2
PDI-3	Protection des documents et des informations	*	Les systèmes d'infomation utilisés dans l'unité doivent être référencés et leur niveau de sensibilité évalué (peu sensible, sensible, très sensible, critique)	7	Gestion des actifs	7.1.1
PDI-4	Protection des documents et des informations	**	Les systèmes informatiques (serveurs, ensemble de serveurs, matériels scientifiques, postes de travail,etc.) utilisés dans l'unité doivent être identifiés et protégés suivant leur niveau de sensibilité	7	Gestion des actifs	7.1.3

☑	PDI-5	Protection des documents et des informations	***	Les systèmes informatiques critiques utilisés dans l'unité doivent être attribués suivant une procédure formelle incluant la signature d'un acte d'engagement de la personne qui en est responsable.	7	Gestion des actifs	7.1.2,
☑	PDI-6	Protection des documents et des informations	**	Les recherches sur Internet pouvant conduite à la divulgation d'informations sensibles dans le cadre de l'intelligence économique doivent être effectués avec des outils limitant la fuite d'informations.	7	Gestion des actifs	
☑	GRH-1	Ressources humaines	*	Le personnel entrant dans l'unité doit être accueilli suivant une procédure d'accueil formalisée qui inclut la prise de connaissance de la charte SSI et des règles élémentaires de sécurité informatique avant l'ouverture des accès sur le SI.	8	Sécurité liée aux ressources humaines	8.1.3
☑	GRH-1-1	Ressources humaines	**	Toute personne physique ou morale amenée à travailler avec l'unité doit signer une clause de confidentialité.	8	Sécurité liée aux ressources humaines	6.1.5
☑	GRH-1-2	Ressources humaines	***	L'aptitude à respecter les règles de sécurité est prise en considération lors du recrutement du personnel sur des postes de confiance.	8	Sécurité liée aux ressources humaines	8.1.2
☑	GRH-1-3	Ressources humaines	*	Les personnes qui ne font pas partie du personnel doivent prendre connaissance des règles SSI de l'unité avant toute connexion au SI de l'unité	8	Sécurité liée aux ressources humaines	
☑	GRH-2	Ressources humaines	*	Le personnel sortant de l'unité doit être connu de l'équipe informatique qui applique une procédure de départ formalisée incluant la fermeture des droits sur le SI et la restitution des matériels appartenant à l'unité.	8	Sécurité liée aux ressources humaines	8.3.1, 8.3.2, 8.3.3
☑	GRH-3	Ressources humaines	*	Le personnel en déplacement à l'étranger doit suivre, avant son départ, une sensibilisation spécifique aux risques relatifs à ces déplacements.	8	Sécurité liée aux ressources humaines	8.2.2
☑	GRH-4	Ressources humaines	**	Le personnel en déplacement à l'étranger doit suivre une procédure formalisée permettant une gestion des matériels informatiques spécifique aux risques relatifs à ces déplacements.	8	Sécurité liée aux ressources humaines	8.2.2
☑	PHY-1	Sécurité physique	*	Un plan détaillé des locaux doit permettre d'identifier les locaux et/ou des zones sensibles (locaux ou zones qui contiennent des matériels, informations ou SI sensibles) qui seront marqués suivant leur niveau de sensibilité.	9	Sécurité physique et environnementale	9.1.1

☑	PHY-2	Sécurité physique	*	Les locaux et/ou zones doivent être protégés par les moyens recommandés suivant leur niveau de sensibilité(peu sensible, sensible, très sensible, critique).	9	Sécurité physique et environnementale	9.1.3
☑	PHY-2-1	Sécurité physique	***	L'intervention des personnels et des visiteurs dans les zones sécurisées (zone 3 et zone 4) est encadrée par des procédures suivant les directives nationales.	9	Sécurité physique et environnementale	9.1.5
☑	PHY-2-2	Sécurité physique	***	Des moyens de protection contre les accès physiques illicites sont définis et mis en œuvre pour chacune des zones suivant les directives nationales.	9	Sécurité physique et environnementale	9.1.2
☑	PHY-2-3	Sécurité physique	***	La procédure de sortie d'un matériel qui est extrait d'une zone de niveau supérieur à 2 doit suivre les directives nationales.	9	Sécurité physique et environnementale	9.2.7
☑	PHY-3	Sécurité physique	**	Les matériels informatiques sont protégés par une fixation lorsqu'il sont susceptibles d'être facilement emportés.	9	Sécurité physique et environnementale	9.2.1
☑	EXP-1	Exploitation des SI	**	Les procédures d'exploitation des systèmes doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	10	Gestion de l'exploitation et des télécommunications	10.1.1
☑	EXP-2	Exploitation des SI	**	Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans le système d'information en exploitation.	10	Gestion de l'exploitation et des télécommunications	10.1.4
☑	EXP-3	Exploitation des SI	*	Lorsque tout ou partie de l'exploitation des SI est confiée à un tiers, Il doit être assuré que les mesures de sécurité définies par cette politique sont reportées dans le contrat.	10	Gestion de l'exploitation et des télécommunications	10.2.1
☑	EXP-4	Exploitation des SI	*	L'usage d'outils permettant d'administrer à distance un système ou permettant d'effectuer des diagnostics techniques est réservé aux seuls administrateurs techniques autorisés.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-5	Exploitation des SI	*	La gestion des traces de l'activité des systèmes informatiques doit suivre les directives nationales	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-5-1	Exploitation des SI	**	Les traces générées par les systèmes informatiques doivent être centralisées et stockées sur 12 mois glissants.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-6	Exploitation des SI	***	Les systèmes informatiques (serveurs, matériels actifs, etc.) sont supervisés via les outils ad hoc.	10	Gestion de l'exploitation et des télécommunications	

☑	EXP-7	Exploitation des SI	***	Les traces générées par les systèmes informatiques (serveurs, postes de travail, matériels actifs, etc.) sont régulièrement analysées pour détecter d'éventuels évènements anormaux.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-8	Exploitation des SI	*	Les systèmes d'acquisition et de contrôle des données (SCADA, Supervisory Control And Data Acquisition) doivent être traités comme des SI à part entière en fonction de leur sensibilité.	10	Gestion de l'exploitation et des télécommunications	7.1.1, 7.1.3
☑	EXP-CNF-1	Exploitation des SI	*	Le parc logiciel de l'unité est géré et permet notamment un suivi de l'attribution des logiciels au personnel.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-CNF-2	Exploitation des SI	**	Les logiciels (OS, applications, etc.) utilisés par le personnel doivent faire partie de la liste des logiciels autorisés par le CSSI de l'unité.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-CNF-3	Exploitation des SI	*	La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-MAT-1	Exploitation des SI	**	Le parc du matériel informatique de l'unité est géré et permet notamment un suivi de l'attribution de ces matériels au personnel.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-MAT-2	Exploitation des SI	**	L'utilisation du matériel informatique est soumise à une autorisation préalable	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-MAT-4	Exploitation des SI	**	La maintenance du matériel informatique doit suivre une procédure formalisée permettant de protéger les informations manipulées par ce matériel.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-MAT-4-1	Exploitation des SI	**	La mise au rebut d'un matériel sensible doit suivre les directives nationales.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-RES-1	Exploitation des SI	**	Un plan détaillé du réseau de l'unité doit permettre d'identifier les zones sensibles (segment de réseau contenant des SI sensibles) qui seront marqués suivant leur niveau de sensibilité (peu sensible, sensible, très sensible, critique).	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-RES-2	Exploitation des SI	**	Les zones sensibles du réseau doivent être protégées par les moyens recommandés suivant leur niveau de sensibilité.	10	Gestion de l'exploitation et des télécommunications	
☑	EXP-RES-4	Exploitation des SI	**	Les dispositifs de contrôle des accès au réseau et aux zones sensibles de ce réseau doivent traiter de façon différenciée les accès des postes de travail contrôlés des accès de postes non contrôlés.	10	Gestion de l'exploitation et des télécommunications	

☑	EXP-RES-6	Exploitation des SI	*	La prise de main à distance sur un poste de travail ne peut être réalisée que par des administrateurs autiorisés et sous le contrôle de l'utilisateur habituel de ce poste de travail.	10	Gestion de l'exploitation et des télécommunications	
☑	AUT-1	Authentification et contrôle d'accès	*	Seuls les comptes individuels (non partagés) sont autorisés pour l'identification préalable à l'accès aux ressources informatiques (postes de travail, systèmes d'information, etc.).	11	Contrôle d'accès	11.1.1
☑	AUT-2	Authentification et contrôle d'accès	*	Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI, qu'elle soit locale ou nationale, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé qui s'appuie sur le processus d'entrée et de sortie du personnel.	11	Contrôle d'accès	11.2.1
☑	AUT-2-1	Authentification et contrôle d'accès	***	Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI classée ZRR doit être gérée suivant les directives nationales.	11	Contrôle d'accès	
☑	AUT-4	Authentification et contrôle d'accès	*	La gestion des moyens d'authentification des utilisateurs sur les SI doit se faire suivant les recommandations nationales	11	Contrôle d'accès	
☑	AUT-5	Authentification et contrôle d'accès	*	Lorsque les moyens de contrôle d'accès personnels d'un utilisateur aux informations doivent être rendus accessibles aux administrateurs, l'utilisateur doit en être informé et ces informations doivent transmises et stockées de façon sécurisée.	11	Contrôle d'accès	
☑	AUT-8	Authentification et contrôle d'accès	***	Le contrôle d'accès aux SI classés ZRR est géré suivant les directives nationales.	11	Contrôle d'accès	
☑	DEV-1	Développement des SI	**	Tout projet informatique/scientifique doit respecter les exigences nationales en matière de sécurité des Systèmes d'Information et prendre en compte la sécurité dès son démarrage.	12	Acquisition, développement et maintenance des systèmes d'information	
☑	INC-1	Gestion des incidents	*	Tout incident de sécurité doit être géré suivant la procédure formalisée par le RSSI du CNRS (qualification, protection, alerte, etc.).	13	Gestion des incidents liés à la sécurité de l'information	
☑	CNT-1	Continuité d'activité	*	Un plan de sauvegarde informatique de l'unité doit être formalisé et mis en œuvre de façon à garantir la récupération des données en cas de sinistre ou de panne matérielle et/ou logicielle sur les matériels gérés par l'unité.	14	Gestion de la continuité de l'activité	15.2.1, 15.2.2

☑	CNT-2	Continuité d'activité	**	Un plan de continuité d'activité doit être formalisé en fonction des besoins de l'unité en la matière.	14	Gestion de la continuité de l'activité	
☑	CNF-1	Conformité	*	Le DU est responsable de l'application des procédures liées à la mise en œuvre de la réglementation relative au traitement automatisé des données à caractère personnel réalisés sur des systèmes qui sont sous la responsabilité de l'unité.	15	Conformité	15.1.4
☑	CNF-2	Conformité	*	Le DU est responsable du suivi du bon respect des règles en matière de protection des données à caractère personnel pour l'ensemble des traitements dont son unité est responsable.	15	Conformité	15.1.4
☑	CNF-3	Conformité	*	Le DU s'assure de la mise en œuvre de moyens de prévention visant à interdire la consultation et la diffusion de messages à caractère violent, pédo-pornographique ou de nature à porter atteinte à la dignité humaine.	15	Conformité	15.1.5
☑	CNF-4	Conformité	*	Le DU s'assure du respect des droits de propriété intellectuelle pour tout logiciel, support multimédia (photos, fichiers audio et vidéo, etc.), base de données ou document manipulé au sein de son unité.	15	Conformité	15.1.2
☑	CNF-5	Conformité	**	Le DU doit transmettre chaque année, via le RSSI de DR, un rapport au FSD et au RSSI du CNRS permettant de juger du niveau d'application des règles de sécurité des SI dans l'unité.	15	Conformité	
☑	CNF-6	Conformité	*	Le DU doit mettre à disposition de l'audit interne du CNRS, du RSSI du CNRS, du RSSI de la DR dont il dépend tout document permettant de juger du niveau d'application des règles de sécurité des SI dans l'unité.	15	Conformité	15.3.1