Annexe à la P591
Prescriptions minimales pour la réalisation organisationnelle e technique

Annexe à la Prescription sur la cyberprotection et la sécurité des données, aux instructions pour les systèmes rattachés à la plate-forme NOVA et leurs utilisateurs

Édition du 28.04.2025

Modifications valables à partir du 1.07.2025 (v1.4)

Chapitre/chiffre	Modifications
12, 13, 31, 32	Précision des formulations en cas de cryptage lors de la transmission ou du stockage
Glossaire, 6, 10, 12, 13, 16, 17, 19, 23, 27, 31, 32	Précision des formulations
11	Délai de conservation réduit de 2 ans à 6 mois
19	Précision du terme "contrat" à "au moins l'annexe 12 de l'Ue500"
14	X ajouté pour Lm
ensemble du document	Ajouts et précisions afin d'améliorer la compréhension

Alliance SwissPass Länggassstrasse 7 3012 Berne Tél. +41 31 359 22 40
info@allianceswisspass.ch allianceswisspass.ch

Table des matières

Remarques préliminaires

Généralités et but

La présente annexe à la P591 sur la cyberprotection et la sécurité des données décrit les standards organisationnels et techniques minimaux à respecter pour le rattachement à l'environnement du système NOVA. Toute convention y dérogeant doit être documentée de manière compréhensible et transparente. La dérogation doit être examinée et justifiée au moins une fois par an, et adaptée dès que possible pour répondre aux standards.
Outre la P591, les réglementations suivantes valent en particulier en matière de cyber-protection et de sécurité des données :

- Conditions d'utilisation de NOVA (C500, annexe 12)
- Réglementation sur l'utilisation des données dans les TP (C500, annexe 16)

Les entreprises de transport (ET) qui ne sont pas membres du SDN, ainsi que les tiers, doivent également conclure un contrat standard. Ce contrat stipule que les exigences de la P591 leur sont également applicables, à moins qu'ils ne soient déjà soumis à la C500.

- Contrat standard NOVA pour les tiers et les ET non membres du SDN

Contexte (sécurité de l'information)

Les exigences suivantes posées à la sécurité de l'information sont conçues selon un principe de niveaux- et doivent être adaptées aux prestations NOVA selon les groupes d'utilisateurs.
Si un utilisateur NOVA est classé dans diverses catégories par l'exploitant NOVA, il doit remplir les exigences du niveau le plus élevé.
Les utilisateurs lecteurs obtenant des données personnelles ont le droit d'utiliser des données de l'environnement NOVA aux finalités définies dans la convention d'utilisation de NOVA.

Les catégories suivantes divergent par leurs exigences et impliquent la réalisation plus ou moins détaillée de mesures :

Lecture sans obtention univoque de données personnelles (Lo) :
Les utilisateurs lecteurs de NOVA n'obtenant pas de données personnelles traitent en principe uniquement des informations pseudonymisées de NOVA permettant de remonter aux personnes exclusivement aux divisions habilitées de l'exploitant NOVA.

Lecture avec obtention univoque de données personnelles (Lm) :
Les entreprises traitant des données à caractère personnel sont impérativement soumises à une convention d'utilisation et doivent remplir des prescriptions de protection des données.

Lecture/écriture (L/S) :
Les utilisateurs lecteurs et auteurs de NOVA peuvent en sus modifier des données au sein de l'environnement NOVA.

Glossaire

Alliance SwissPass	Organisation de la branche des transports publics, regroupant 250 entreprises de transport et 20 communautés, s'engageant au niveau suisse pour des dispositions tarifaires harmonisées, compréhensibles et économiques, des solutions de distribution modernes et attrayantes et des assortiments et systèmes d'information axés sur la clientèle.
Attaque DDoS	Lors d'une attaque par déni de service distribué (DDoS – Distributed Denial of Service), un attaquant submerge un site web, un serveur ou une ressource réseau avec un trafic extrêmement élevé, dans le but de provoquer son arrêt ou de limiter sa disponibilité.
API (Application Programming Interface)	Interface de programmation qui permet à des programmes logiciels de communiquer entre eux et d'échanger des données.
CA (Certificate Authority), - Autorité de certification	Une autorité de certification, également appelée instance de certification, est une entité organisationnelle en sécurité de l'information qui émet des certificats numériques dans le cadre d'une infrastructure à clé publique (PKI). Il existe des autorités de certification publiques et internes aux entreprises.
C500, Convention 500	Contrat de collaboration de la branche réglant les compétences au sein de l'Alliance SwissPass, régulièrement mis à jour
CIS, niveau 1	Abréviation de « Center for Internet Security », une organisation d'utilité publique promouvant la cybersécurité. Le niveau 1 représente une configuration de sécurité de base et est perçu comme un standard minimal. Les contrôles du niveau 1 visent à couvrir les principaux vecteurs de menace et à protéger le système des attaques les plus courantes. Les directives du niveau 1 sont moins restrictives et offrent un bon équilibre entre sécurité et fonctionnalité du système. Le niveau 1 est approprié pour la plupart des environnements et recommandé pour garantir un niveau de sécurité fondamental.
CISO	Abréviation de « chief information security officer », responsable de la sécurité des systèmes d'information en français.
Contrôle d'intégrité	Garantie et traçabilité de l'intégrité et de l'exhaustivité des informations au moyen de la journalisation (« logging ») et de la sauvegarde inaltérable des données.
CVSS Niveau 7	Le « Common Vulnerability Scoring System » est une norme industrielle développée par FIRST pour évaluer le niveau de gravité des vulnérabilités potentielles ou effectives dans les systèmes informatiques. Les mesures ou niveaux mentionnés ici se réfèrent aux spécifications de la version 3 (CVSS v3).
Cyberprotection	Ensemble de mesures visant à protéger des ordinateurs, des serveurs, des appareils mobiles, des systèmes électroniques, des réseaux et des données contre toute attaque malveillante du cyberespace.
Droits privilégiés	Les comptes avec des droits privilégiés sont généralement des comptes d'administrateurs informatiques ou d'autres comptes utilisateurs disposant de droits ayant un fort impact opérationnel. Ils ont souvent accès à des fonctions système critiques et peuvent apporter des modifications significatives à l'état de fonctionnement, aux configurations et aux données des systèmes. Ils sont soumis à des exigences de sécurité particulières, qu'ils doivent impérativement respecter.
Exploitant NOVA	Mandataire chargé par l'Alliance SwissPass de l'exploitation des systèmes et infrastructures de NOVA
Filtrage des applications web	Logiciel restreignant l'accès aux applications, sites Internet et contenus dangereux.

FIRST	FIRST signifie « Forum for Incident Response and Security Teams » (www.first.org) et agit en tant qu'administrateur des spécifications CVSS.
Framework	Le terme « framework » est un synonyme de cadre ou de structure de base.
Infrastructure à clé publique (PKI)	L'infrastructure à clé publique (Public Key Infrastructure – PKI) est un système hiérarchique destiné à l'émission, à la distribution et à la vérification de certificats numériques. Ces certificats numériques permettent d'établir une association fiable entre des entités et leurs clés publiques.
Intermédiaire(s)	Organisation(s) vendant des assortiments NOVA en représentation d'une ou de plusieurs entreprises de transport prestataires. Le terme comprend les entreprises de transport au titre d'une concession de l'OFT, les gestionnaires d'une infrastructure ferroviaire, les communautés tarifaires et de trafic et les tiers rattachés à NOVA.
Maliciel (*malware*)	Terme générique désignant les logiciels malveillants développés pour infiltrer les appareils en toute discrétion, provoquer des dommages ou des interruptions ou voler des données. Ce terme comprend les publiciels (*adwares*), les logiciels espions (*spywares*), les virus, les botnets, les chevaux de Troie, les vers informatiques, les rootkits et les rançongiciels.
NIST	Le cadre de cybersécurité du National Institute of Standards and Technology (NIST) des États-Unis (www.nist.gov) fournit des directives complètes et des meilleures pratiques permettant aux entreprises d'améliorer leur gestion des risques en matière de sécurité de l'information et de cybersécurité.
Objet à protéger	Tout système, application, réseau, recueil de données, infrastructure et produit traitant des données NOVA.
OFT	Office fédéral des transports
Organe de gestion de l'Alliance SwissPass	Organe gérant les affaires de l'Alliance SwissPass selon la Convention 500.
Pare-feu à états « Stateful Firewalling »	L'inspection dynamique des paquets (Stateful Packet Inspection) est une technique de filtrage des paquets dans laquelle chaque paquet de données est associé à une session active spécifique. Les paquets sont analysés et l'état de la connexion est pris en compte dans le processus décisionnel en cours.
Plateforme NOVA	Plateforme nationale de distribution des titres de transport des transports publics suisses. De l'allemand « Netzweite ÖV-Anbindung ».
Prestataire	Personne physique (être humain habilité en droit) ou morale (entreprise, organisation, etc.) fournissant une prestation.
Principe de niveaux	Principe selon lequel les utilisateurs NOVA classés dans plusieurs/diverses catégories par l'exploitant NOVA doivent remplir les exigences du niveau le plus élevé.
Propriétaire de tarif	Instance exerçant la souveraineté tarifaire (Service direct national [SDN], service direct régional [communauté tarifaire ou de trafic], entreprise de transport).
Protocole cryptographique/de chiffrement	On distingue les protocoles destinés au stockage ou au transport. Il existe de plus différentes fonctions de cryptographie sur la base d'un chiffrement, d'une signature ou d'une somme de contrôle afin de pouvoir vérifier l'intégrité d'informations techniques : - AES 256 bits : l'Advanced Encryption Standard (AES) est un algorithme de cryptographie symétrique recourant à une clé de 256 bits pour chiffrer du texte ou des données. - RSA : protocole de cryptographie asymétrique utilisé pour chiffrer et pour signer numériquement.

	- Fonction de hachage cryptographique : utilisée pour vérifier l'intégrité de fichiers ou de messages et indique à l'aide d'une valeur cryptographique annexée (hachage) si une modification a été apportée. Également employée dans les signatures numériques et les vérifications de mots de passe. - SHA2 / SHA 3 : abréviation de « Secure Hash Algorithm », existe en plusieurs versions et met des fonctions de hachage à disposition pour identifier des valeurs de contrôle univoques de données numériques. - Échange de clés Diffie-Hellman : protocole permettant à deux partenaires de communiquer secrètement sur un canal public interceptable grâce à une clé commune, sous forme d'un nombre, qu'eux seuls connaissent et que personne d'autre ne peut identifier. - Suites cryptographiques TLS : il s'agit du protocole Transport Layer Security (TLS) et de son prédécesseur Secure Socket Layer (SSL). Les suites cryptographiques sont une suite d'algorithmes employés pour sécuriser des connexions réseau entre des clients et des serveurs. Les protocoles TLS/SSL sont utilisés notamment dans la conception d'HTTPS, de FTPS, de POP3, de SMTPS et d'autres protocoles. - RC4 (Rivest-Chiffre 4) : chiffrement de flux, chiffrant des messages octet par octet à l'aide d'un algorithme. - DES (Data Encryption Standard) : algorithme cryptographique symétrique très répandu. - IDEA (International Data Encryption Algorithm): chiffrement par bloc symétrique. - ECB (Electronic Code Book Mode) : type d'exploitation pour les chiffrements par bloc. - HMAC : code d'authentification par message obtenu en exécutant une fonction de hachage cryptographique (telle MD5, SHA1 et SHA256) sur les données à authentifier en combinaison avec une clé secrète commune.
Standard minimal pour les TIC	« Norme minimale pour améliorer la résilience informatique » de l'Office fédéral de l'approvisionnement économique du pays (OFAE)
Système de détection d'intrusion	Système visant à identifier les attaques menées contre un système informatique ou un réseau d'ordinateurs.
TCP/IP	Abréviation de « Transmission Control Protocol/Internet Protocol », soit un groupe de protocoles réseaux. Dans le noyau, il s'agit de l'Internet Protocol (IP), du Transmission Control Protocol (TCP), du User Datagram Protocol (UDP) et de l'Internet Control Message Protocol (ICMP). Plus généralement, toute la suite des protocoles Internet est nommée TCP/IP.
Tiers	Organisations qui se raccordent à la plateforme NOVA et utilisent l'assortiment NOVA, mais qui ne sont ni des entreprises de transport concessionnées par l'OFT, ni des gestionnaires d'infrastructure ferroviaire, ni des communautés tarifaires et/ou de transport suisses.
Top 10 OWASP	Abréviation de « Open Web Application Security Project », soit une organisation à but non lucratif dédiée à la sécurité des applications web. Le top 10 est un rapport régulièrement actualisé qui décrit les problèmes de sécurité des applications web et se concentre sur les dix risques les plus critiques.
TP	Transports publics
Transporteur(s)	Prestataire(s) réalisant des transports physiques (p. ex. une entreprise de transports publics ou un taxi) ou exploitant une infrastructure ou un véhicule qu'il possède (p. ex. Mobility). S'y ajoutent toujours plus d'« intermédiaires » proposant non pas directement de services de mobilité, mais des offres correspondantes en les combinant parfois (p. ex. Whim, moovel).

Utilisateurs NOVA	L'ensemble des utilisateurs de la plateforme NOVA, soit les intermédiaires, les transporteurs, les propriétaires de tarif et les prestataires.
Vente	On entend par « vente » l'ensemble du processus de vente de titres de transport des transports publics, commençant par l'information et le conseil au voyageur, suivi par la vente en tant que telle et le paiement, et incluant encore le contrôle et le service après-vente (échange, annulation, remboursement, réclamation).
Zero-day	Terme générique pour désigner les lacunes de sécurité nouvellement identifiées par lesquelles des hackers peuvent attaquer des systèmes. L'expression en anglais se rapporte au fait que le fabricant ou le développeur découvre l'erreur au moment de l'attaque et a donc « zéro jour » pour la résoudre. On parle d' « attaque zero-day » lorsque les hackers peuvent exploiter la faille avant que les développeurs n'aient pu l'éliminer.
Zone démilitarisée (DMZ)	Réseau d'ordinateurs avec des possibilités d'accès contrôlées techniquement aux serveurs qui y sont raccordés. Les systèmes de la zone démilitarisée sont protégés contre d'autres réseaux par un ou plusieurs pare-feu et d'autres mesures techniques de sécurité.

Prescriptions minimales sur la base du standard minimal pour les TIC

<table>
<tr><th>Lo</th><th>Lm</th><th>L/S</th><th>Exigences</th><th>Norme min. TIC</th></tr>
<tr><td>X</td><td>X</td><td>X</td><td>1. Inventaire des objets à protéger

Les objets à protéger et leurs composants doivent être listés dans le détail dans un inventaire.
Les modifications des objets à protéger doivent être reportées dans l’inventaire.
L’actualité de celui-ci doit être vérifiée chaque année.
Les objets à protéger devenus inutiles ou qui ne sont plus exploités doivent être supprimés de l’inventaire.</td><td>ID.AM-1
PR.DS-3</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>2. Analyse du besoin de protection

Une analyse du besoin de protection doit être réalisée pour chaque objet à protéger. Les critères de confidentialité, d’intégrité et de disponibilité doivent être évalués selon au moins trois niveaux.
<table>
<tr><th></th><th>Confidentialité</th><th>Intégrité</th><th>Disponibilité</th></tr>
<tr><td>Pas d’exigences</td><td>public</td><td>pas d’exigences</td><td>Sous la responsabilité de l’utilisateur NOVA</td></tr>
<tr><td>Exigences standard</td><td>interne</td><td>compréhensible</td><td>Sous la responsabilité de l’utilisateur NOVA</td></tr>
<tr><td>Exigences élevées</td><td>confidentiel</td><td>démontrable</td><td>Sous la responsabilité de l’utilisateur NOVA</td></tr>
</table>
Les disponibilités de l’exploitant NOVA ne font pas partie de cette annexe.</td><td>ID.AM-5
ID.BE-4</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>3. Matrice de communication

Pour chaque objet de protection lié à NOVA, les flux de communication et de données doivent être documentés.
La relation de communication crée de la transparence et donne un aperçu :

• de quels systèmes / applications / utilisateurs
• par quels protocoles
• et par quels ports

on accède à d’autres systèmes / applications.</td><td>ID.AM-3
ID.AM-4</td></tr>
<tr><td></td><td>X</td><td>X</td><td>4. Sécurité physique

Les systèmes et infrastructures IT doivent être protégés par des mesures physiques/architecturales selon leur besoin de protection. On veillera en particulier à ce que seules des personnes autorisées aient un accès physique ou un accès à l’objet à protéger.</td><td>PR.AC-2</td></tr>
</table>

X	X	X	**5. Comptes utilisateurs - logins des utilisateurs NOVA** Les accès utilisateurs (« logins ») attribués directement à NOVA ou à des systèmes fournisseurs pour l'utilisation d'objets protégés doivent respecter les exigences suivantes : • Les utilisateurs de NOVA sont tenus d'ouvrir un compte utilisateur personnel pour chaque collaborateur/trice requérant l'accès à NOVA. Les comptes partagés par groupe ne sont pas autorisés. • Les utilisateurs NOVA veillent à ce que les comptes personnels ne soient utilisés par aucune autre personne. • Les utilisateurs tiennent un registre de tous les comptes et garantissent l'identification du titulaire de chaque compte. • Les utilisateurs de NOVA sont tenus de communiquer à l'exploitant de NOVA, à sa demande, quelle personne physique utilise un compte ainsi que les rôles (administrateur/ accès technique, etc.) qui lui ont été attribués. • Des processus et des mesures techniques sont établis pour l'octroy, la gestion et la révocation des autorisations pour les utilisateurs et les appareils. • Les droits comportent tous les types d'accès, soit les accès physiques, de système et à distance. • L'accès doit être protégé par une authentification à facteurs multiples (MFA). • Les utilisateurs de NOVA disposant de droits privilégiés doivent, au minimum une fois, vérifie l'identité de leurs collaborateurs/trices sur la base d'un document officiel d'identité valable tel qu'un passeport ou une carte d'identité, et contrôler de manière récurrente leur intégrité au moyen d'extraits officiels récents du casier judiciaire ou de l'office des poursuites.	PR.AC-1 PR.AC-6
X	X	X	**6. Comptes et logins techniques** Les logins techniques de systèmes rattachés à NOVA doivent satisfaire les exigences suivantes : • Les comptes doivent être uniques et exclusivement attribués à une fonction ou à un service technique. • Les comptes sont univoquement attribués à un utilisateur, soit une personne physique responsable • Les utilisateurs ne doivent disposer que des privilèges nécessaires à la fonction ou au service requis. • Le mot de passe doit être modifié à chaque changement majeur de version (release), au minimum une fois par an.	PR.AC-1 PR.AC-2 PR.AC-4 PR.AC-6

X	X	X	**7. Gestion des mots de passe** Les objets à protéger doivent systématiquement demander des mots de passe forts : • Une exigence minimale en matière de mot de passe (cf. exigence 8) est définie dans le système et impose automatiquement les critères suivants : • Les mots de passe ne doivent pas être employés deux fois. • Les mots de passe doivent être cryptés ou hachés. • Le stockage de mots de passe sous forme de texte en clair est interdit. • Les mots de passe ne doivent pas être transmis. Il doit être garanti au niveau du système que les mots de passe initiaux/par défaut doivent être modifiés lors de la première connexion. Pour réinitialiser des mots de passe oubliés, échus ou bloqués, un processus documenté doit être mis en œuvre pour chaque objet à protéger.	PR.IP-1
X	X	X	**8. Exigences relatives aux mots de passe** Les mots de passe des objets à protéger doivent satisfaire les exigences suivantes : • Longueur minimale : 12 caractères • Composition alphanumérique, avec des majuscules et des minuscules • Pas de mots de dictionnaires	PR.IP-1
		X	**9. Accès à distance** Sur les objets à protéger, les accès aux données NOVA ne passant pas par des réseaux propres à NOVA doivent satisfaire aux prescriptions standard du mandataire. Un accès temporaire est accordé à des tiers. Les accès et leurs droits doivent être documentés, régulièrement contrôlés et limités au strict nécessaire (principe de moindre privilège). Les sous-traitants doivent également satisfaire ces exigences. Pour la maintenance à distance, des comptes utilisateurs personnalisés doivent être mis en place. Ceux-ci doivent être surveillés, protégés (MFA) et leur utilisation doit être documentée de manière traçable (journalisation).	PR.AC-3 PR.MA-2

X	X	X	**10. Journalisation des objets à protéger** La journalisation et son étendue doivent être définies pour tout objet à protéger avec le responsable de la sécurité de l'information/CISO. Les activités suivantes doivent en principe être enregistrées et surveillées sous une forme pseudonymisée pour les objets protégés, dans un but précis et de manière compréhensible : • Allumage et extinction du système • Processus de connexion • Accès à distance • Échecs d'accès • Octroi et modification de privilèges • Toutes les actions requérant des privilèges élevés • Modifications du système Les données de journalisation doivent être analysées, centralisées, conservées pendant six mois et évaluées. Les fichiers journaux doivent être protégés contre des manipulations ultérieures.	PR.MA-1 PR.MA-2 PR.PT-1 DE.AE-1 DE.AE-5 DE.CM-1 DE.CM-2 PR.DS-5
X	X	X	**11. Journal de trafic des accès de réseau** Tous les journaux de trafic (logfiles et proxy-logs) d'accès de réseau (pare-feux et gateways) en lien avec NOVA doivent être conservés six mois et évalués dans les règles. Les logs doivent être protégés contre toute manipulation ultérieure. En cas d'utilisation de services NOVA dans l'état contractuel L/S, toutes les données de trafic doivent être activement surveillées par monitoring et faire l'objet d'un processus analytique en cas d'anomalies.	PR.MA-1 PR.MA-2 PR.PT-1
X	X	X	**12. Cryptage des données en transit** Tous les accès aux objets protégés doivent être cryptés lors de la transmission. Le cryptage doit être effectué conformément à l'état actuel de la technique (voir clause 13).	PR.DS-2

X	X	X	**13. Procédures de cryptage** Si un cryptage est exigé, seuls des procédés de cryptage reconnus et contrôlés avec une génération de clé sûre peuvent être utilisés pour les objets protégés et les mots de passe. Une longueur minimale de clé, comme décrite ci-dessous, doit être respectée. Actuellement, les procédures suivantes sont autorisées : • Cryptage symétrique : AES 256 bits • Cryptage asymétrique : RSA avec une longueur d'au moins 2048 bits et les procédures similaires • Fonction de hachage cryptographique : SHA2 ou SHA3 avec au moins 256 bits • Échange de clés : Diffie-Hellman avec au moins 2048 bits ou des méthodes comparables. En cas d'utilisation de suites cryptographiques (*cipher suites*) en TLS, les suites proposées doivent être limitées aux algorithmes sûrs. Ne sont plus considérés comme sûrs : • les algorithmes de cryptage RC4, DES, IDEA • le mode de cryptage ECB • les fonctions de hachage MD4, MD5, SHA-1 (sauf HMAC) • des clés d'une longueur inférieure à 128 bits dans les algorithmes symétriques Ces exigences valent pour le stockage et la transmission de données.	PR.DS-2
X	X	X	**14. Utilisation de certificats** Les accès web aux objets à protéger doivent se faire avec un cryptage de transport TLS. Les règles suivantes s'appliquent : • Les accès web de tiers aux objets à protéger doivent passer par un certificat TLS public valable. • Les accès aux objets à protéger à la disposition d'un cercle de personnes clairement défini, peuvent être effectués à l'aide d'un certificat émis par la CA interne. Les certificats TLS doivent être obtenus auprès d'une autorité de certification (CA) publique reconnue, conformément à un processus défini. Si un objet à protéger dépend de certificats client (p. ex. pour l'authentification d'appareils mobiles), ces certificats doivent être signés par la CA interne et au besoin établis par cette dernière. Les certificats peuvent avoir une durée de validité de deux ans au maximum.	PR.DS-2
	X	X	**15. Élimination de données et d'informations** Si des objets à protéger ou des parties d'entre eux sont remplacés, supprimés ou mis hors service, toutes les données relatives aux services NOVA (p. ex. disques durs) doivent être entièrement supprimés de manière irréversible ou détruits physiquement de façon non récupérable.	PR.IP-6 PR.DS-3

	X	X	**16. Scans de vulnérabilité** Avant leur mise en service et en cas de toute modifications importantes (cf. exigence 22), tous les objets à protéger doivent être examinés (scannés). Les lacunes repérées doivent être signalées aux responsables internes (par exemple les responsables de la sécurité de l'information – ISO, CISO, etc.) et résolues immédiatement. En règle générale : Critique, 9.0 - 10.0 --> immédiatement/avant GoLive • - Les lacunes avec un niveau CVSS v3 de 9.0 à 10.0 et un potentiel de dommages critiques doivent être corrigées immédiatement ou avant le GoLive. High, 7.0 - 8.9 --> Dans les 6 semaines/avant le GoLive • Les lacunes ayant un niveau CVSS v3 de 7.0 à 8.9 et présentant un potentiel de dommages élevé doivent être corrigées dans un délai de 6 semaines ou avant le GoLive.	PR.IP-12 DE.CM-8
	X	X	**17. Tests de pénétration** Avant leur mise en service ou en cas de modifications importantes et lors de grandes mises à jour (cf. exigence 22), les objets à protéger accessibles depuis Internet doivent être examinés au moyen d'un test de pénétration à la recherche de lacunes critiques. Ces tests doivent être réalisés par un organe indépendant. Les services web ne doivent ensuite plus présenter de lacune avec une gravité élevée ou critique selon le standard du top 10 OWASP. Avant leur implémentation, en cas de modifications importantes et lors de grandes mises à jour (cf. exigence 22), les objets à protéger liés à la lecture et à l'écriture doivent être examinés au moyen d'un test de pénétration. Ces tests doivent être réalisés par un organe indépendant.	DE.CM-8
	X	X	**18. Modifications des objets à protéger** Les modifications des objets à protéger doivent être documentées de manière traçable et traitées via un processus de gestion des changements. Les fonctions importantes en matière de sécurité et critiques pour l'exploitation doivent être examinées quant à leur fonctionnement et le cas échéant immédiatement ajustées.	PR.IP-3 PR.DS-6
X	X	X	**19. Prise en compte de la *security baseline* lors de la conclusion du contrat** Les prescriptions minimales de ce document doivent être prises en compte dès la conclusion du contrat, ce qui équivaut ici à l'acceptation de l'annexe 12 de la c500 ainsi que du contrat standard NOVA.	ID.SC-3

	X	X	**20. Séparation de l'exploitation et de l'environnement de test** Lors du développement et de l'essai des objets à protéger, les environnements productif et non productif (staging, testing..) doivent être séparés de sorte que le développement et les tests n'entraînent aucune restriction dans l'environnement productif.	PR.DS-7
	X	X	**21. Prise en compte des standards de sécurité du développement logiciel** Lors du développement d'applications, des standards de sécurité reconnus (p. ex. top 10 OWASP pour le développement web ou NIST SP 800-218 pour le développement logiciel) doivent être appliqués.	PR.IP-1
	X	X	**22. Utilisation de données tests fictifs** Les tests menés dans le cadre du développement et de la mise à disposition d'applications doivent être effectués seulement avec des données fictives.	PR.DS-7
	X	X	**23. Interfaces utilisateurs et API** Si des interfaces utilisateurs sont implémentées sur les objets à protéger, elles doivent respecter les règles suivantes : • L'input et l'output doivent être validés. • Seules des valeurs explicitement admises (liste blanche) sont autorisées. • Les paramètres cachés, comme des variables, les valeurs d'en-tête et les informations sur les cookies, doivent être validées. • La validation porte sur tous les types d'entrées et de sorties, et également sur les données binaires.	PR.IP-1
	X	X	**24. Élaboration de configurations standard et renforcement du système** Lors de l'implémentation, des configurations standard doivent être établies pour tout objet à protéger. Les mesures de renforcement doivent satisfaire le niveau CIS 1. Elles comprennent, entre autres, les règles suivantes : • Les services inutiles, ne soit pas expressément nécessaires, doivent être désactivés, voire supprimés ou désinstallés si possible. • Les comptes inutiles doivent être désactivés ou supprimés. • Les données temporaires sont automatiquement supprimées lors de la déconnexion. • Les paramètres de sécurité sont gérés de manière centralisée. • Les approbations standard sont désactivées.	PR.IP-1
	X	X	**25. Cryptage des sauvegardes** Les sauvegardes (*backup*) doivent être cryptées.	PR.IP-4

X	X	X	**26. Protection contre les maliciels** Tout objet à protéger doit être protéger contre les logiciels malveillants (maliciels). Tous les objets à protéger interagissant directement avec les utilisateurs doivent disposer d'une solution efficace et actuelle contre les malwares. Ces exigences doivent être respectées également pour les sous-traitants.	DE.CM-4 DE.CM-5 PR.DS-6
	X	X	**27. Contrôle d'intégrité** L'intégrité des transactions liées aux objets à protéger et des informations de login doit être contrôlée en continu afin d'identifier rapidement les modifications indues, les écarts et les éventuelles lacunes. Le contrôle peut être assuré par des journaux d'audit et de transaction. Dans la transmission des données, il convient d'utiliser des procédures qui empêchent la modification des données en cours de transmission grâce au contrôle des valeurs de hachage (par ex. par des procédures TLS).	PR.DS-6
	X	X	**28. Application de patches et mises à jour** Pour tout objet à protéger exploité pour les services NOVA, le suivi des patches et des mises à jour doit être documentée afin d'en garantir l'actualité. Les mises à jour et patches critiques pour la sécurité doivent être installés immédiatement, au plus tard dans les trente jours suivant leur publication. Le responsable de la sécurité de l'information (ISO) ou le CISO du mandataire peut, en cas d'urgence ou d'exceptions justifiées (par exemple, une faille de type « zero-day »), ordonner la distribution et l'installation des correctifs dans un délai de 48 heures, en coordination avec le cocontractant.	PR.IP-2
	X	X	**29. Heure système** L'heure système des objets à protéger doit être synchronisée de manière centralisée.	PR.IP-1
	X	X	**30. Maintenance à distance par des tiers** La maintenance d'objets à protéger effectuée à distance par des tiers doit être contrôlée. Les mêmes règles de gestion des utilisateurs et des droits d'accès s'appliquent que pour les autres utilisateurs.	PR.AC-3 PR.MA-2

	X	X	**31. Concept de zones** Un concept de zones de sécurité doit être établi et tenu à jour pour l'exploitation des objets à protéger. Il doit tenir compte des principes suivants : • Le concept de zones doit contenir chaque zone selon la criticité et la sensibilité de ses objets à protéger. • Les transitions entre zones doivent être restreintes à l'aide de mesures appropriées telles que le pare-feu à états (stateful firewalling), la détection d'intrusion, le filtrage des applications web, etc., afin d'empêcher toute propagation latérale indésirable. • Seuls des protocoles standardisés de la suite TCP/IP peuvent être employés. • Le trafic à partir de réseaux non sécurisés (p. ex. Internet) doit être protégé en sus des attaques par déni de service (DDoS) et des méthodes d'attaque connues à l'aide d'un système de détection des intrusions. De plus, le trafic à partir de et vers des réseaux non sécurisés dans une zone démilitarisée (DMZ) doit être fixé (rupture de protocole). • Chaque objet à protéger doit être placé dans une zone de sécurité appropriée du réseau en fonction de son besoin de protection. Ce positionnement doit être approuvé par le responsable du concept de zones ou le responsable de la sécurité de l'information (ISO).	PR.AC-5 PR.PT-4
	X	X	**32. Vérification de logiciels** Tous les logiciels employés dans les services NOVA en lien avec des objets à protéger doivent être vérifiés et peuvent être obtenus uniquement directement du fournisseur officiel ou de l'un de ses partenaires certifiés. La fiabilité des sources et la protection contre toute modification non autorisée du logiciel doivent être garanties. • L'authenticité et l'intégrité des logiciels employés dans les objets à protéger doivent être garanties par une procédure cryptographique automatisée (signatures, contrôle des hachages). • Les logiciels dont l'authenticité ne peut être contrôlée de manière automatisée doivent être vérifiés manuellement (consulter les valeurs de hachage sur le site Internet du développeur). • Les logiciels open source doivent provenir de sources officielles et fiables, et disposer d'une licence open source correspondante d'une organisation reconnue, comme GPL, MIT, BSD, ASF, MPL, etc.	PR.DS-6
	X	X	**33. Communication logicielle au niveau des réseaux** La communication au niveau réseau doit passer par des ports serveur fixes (TCP/IP). L'utilisation de plages de ports dynamiques n'est pas autorisée.	PR.AC-5

X	X	X	**34. Reprise de fonctionnalités importantes pour la sécurité** La sécurité de la plateforme NOVA est sans cesse améliorée. Ses utilisateurs s'engagent à appliquer les fonctionnalités importantes pour la sécurité immédiatement, au plus tard trois mois après leur mise à disposition dans l'environnement productif. L'exploitant NOVA peut prescrire des délais contraignants différents pour des releases très critiques ou d'une ampleur particulièrement grande.	PR.IP-2