P591

Prescrizione sulle disposizioni in materia di protezione contro i ciber-rischi e sicurezza dei dati per i sistemi collegati alla piattaforma NOVA e i relativi utenti (utenti NOVA)

Edizione 11.12.2023

Modifiche valevoli dal 01.01.2024

Capitolo/cifra	**Modifiche**

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

Alliance Swiss Pass+

Contenuto

0 Osservazioni preliminari

0.1 Aspetti generali e finalità

La presente prescrizione definisce gli standard vincolanti delle prescrizioni in materia di sicurezza delle informazioni per gli utenti della piattaforma NOVA. Per allestire la P591 sono state consultate le raccomandazioni esistenti in materia di cibersicurezza, come lo standard minimo TIC, il «Manuale di cybersicurezza per le imprese di trasporti pubblici» o i framework pertinenti come ISO27001 e NIST.

Su tale base vengono dedotte misure che orientandosi al principio «defense in depth» in relazione alla sicurezza delle informazioni esigono e promuovono l'implementazione tecnica.

Tutte le modifiche contenutistiche rilevanti di questa prescrizione (aggiunte, modifiche, cancellazioni ecc.) sono di competenza della KoV, ai sensi delle direttive sulle competenze, cifra 7 del regolamento organizzativo, C500. Il segretariato dell'Alliance SwissPass è incaricato dell'aggiornamento delle presenti prescrizioni.

Oltre alle P591, in relazione alla protezione contro i ciber-rischi e alla sicurezza dei dati si applicano in particolare anche le seguenti prescrizioni e disposizioni esistenti (elenco non esaustivo):

- Condizioni di utilizzo NOVA (C500 allegato 12)
- Regolamento sull'utilizzo dei dati tp (C500 allegato 16)

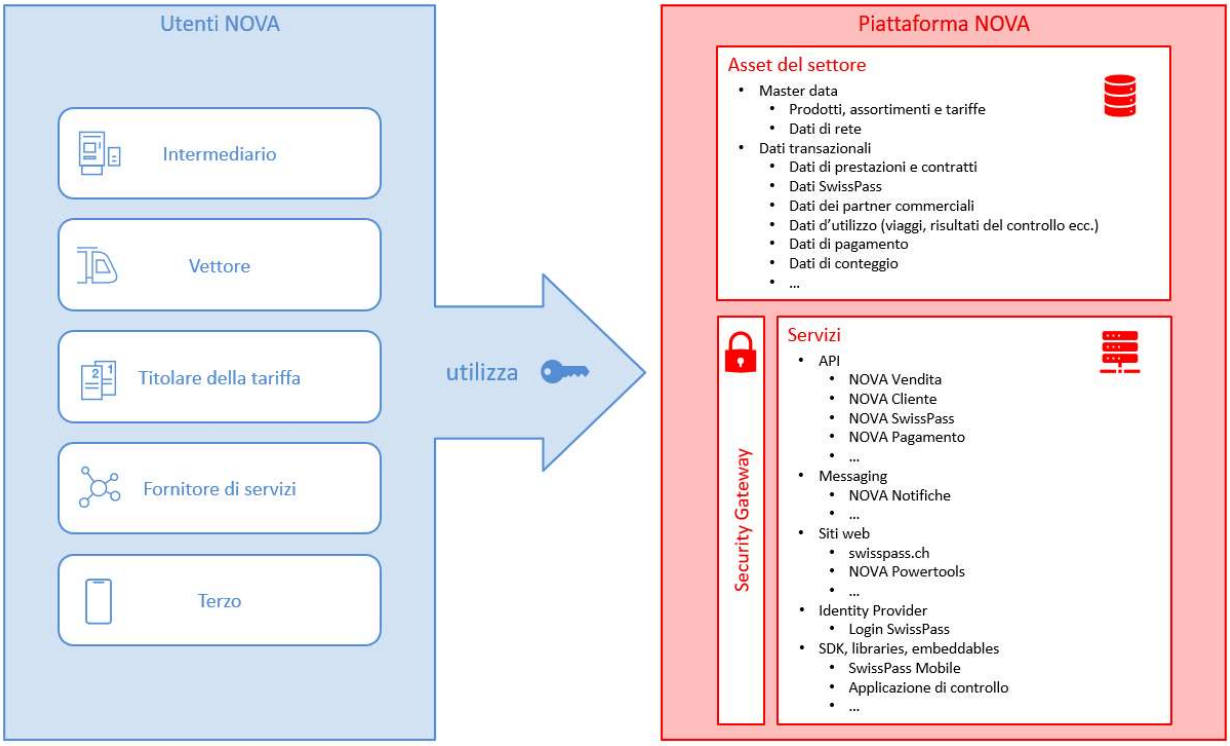
0.2 Glossario

Alliance SwissPass	Organizzazione di settore dei trasporti pubblici formata da 250 imprese di trasporto e 18 comunità, che si impegna a livello nazionale a favore di condizioni tariffarie armonizzate, chiare ed economiche, soluzioni di vendita moderne e allettanti nonché assortimenti e sistemi informativi orientati ai clienti.
C500	La Convenzione 500 (C500), il contratto di collaborazione del settore, disciplina le competenze all'interno dell'Alliance SwissPass.
Comunità	Comunità di abbonamenti, tariffaria o dei trasporti
CU NOVA	Condizioni di utilizzo della piattaforma NOVA, allegato 12 della C500
DE-Oferr	«Disposizioni d'esecuzione dell'ordinanza sulle ferrovie (DE-Oferr)»
FFS	Ferrovie federali svizzere
Fornitore di servizi	Il fornitore di servizi è la persona o l'impresa che eroga la prestazione. Può essere una persona fisica, vale a dire una persona dotata di capacità giuridica, o una persona giuridica (impresa, organizzazione ecc.).
Framework	Framework è un altro termine per indicare il quadro riferimento o la struttura di base; qui sta per direttive o misure.
Gestore NOVA	Mandatario incaricato dall'Alliance SwissPass per la gestione dei sistemi e delle infrastrutture NOVA → Piattaforma NOVA.
Intermediario	Organizzazione che vende assortimenti NOVA in rappresentanza di una o più imprese di trasporto incaricata/e della fornitura di servizi. In questa categoria rientrano le imprese di trasporto titolari di una concessione

	dell'UFT, i gestori di un'infrastruttura ferroviaria, le comunità tariffarie e dei trasporti svizzere e i terzi collegati a NOVA.
ISMS	Un Information Security Management System (ISMS, in italiano «sistema di gestione della sicurezza delle informazioni») è un insieme di procedure e regole all'interno di un'organizzazione che serve a definire, gestire, controllare, mantenere e migliorare in maniera duratura e continua la sicurezza delle informazioni.
ISO 27001	ISO 27001 è uno standard internazionale per la sicurezza delle informazioni.
KoV	Commissione Distribuzione
Livello CVSS 7	«Common Vulnerability Scoring System», uno standard industriale per la valutazione della gravità delle potenziali o effettive vulnerabilità di sicurezza nei sistemi informatici (qui viene utilizzato nella versione 3).
NIST	Il NIST Cybersecurity Framework offre istruzioni complete e best practice che le imprese possono seguire per migliorare la gestione dei rischi per la sicurezza delle informazioni e la cibersicurezza.
Piattaforma NOVA	Piattaforma nazionale per la vendita di titoli di trasporto. Nome del prodotto: «Interfaccia tp su tutta la rete»
Protezione contro i ciber-rischi	Misure per proteggere o difendere computer, server, dispositivi mobili, sistemi elettronici, reti e dati da attacchi intenzionali dal ciberspazio.
Root cause	L'analisi della causa radice (in inglese Root Cause Analysis, in breve RCA) è un processo per determinare la causa profonda dei problemi al fine di trovare soluzioni adeguate.
Segretariato dell'Alliance SwissPass	Il segretariato gestisce le attività dell'Alliance SwissPass secondo le disposizioni della Convenzione 500.
Standard minimo per le TIC	«Standard minimo per migliorare la resilienza delle TIC» dello standard di settore Approvvigionamento economico del Paese.
Terzi	Organizzazioni che aderiscono alla piattaforma NOVA e che distribuiscono l'assortimento NOVA ma che non sono imprese di trasporto che hanno ricevuto una concessione dall'UFT, gestori di un'infrastruttura ferroviaria o comunità tariffarie e/o dei trasporti svizzere.
Titolare della tariffa	L'istanza che esercita il controllo sulla tariffa (Servizio diretto nazionale [SDN], Servizio diretto regionale [comunità tariffarie o dei trasporti], imprese di trasporto).
tp	Trasporti pubblici
UFT	Ufficio federale dei trasporti
Utenti NOVA	L'insieme degli utenti in qualità di intermediari, vettori, titolari della tariffa e fornitori di servizi.
Vendita	Per vendita s'intende l'intero processo di vendita di titoli di trasporto dei trasporti pubblici che inizia con l'informazione/consulenza alla clientela e continua con la vera e propria procedura di vendita, incluso il pagamento. Seguono il controllo dei titoli di trasporto e il servizio dopo vendita (cambio, annullamento, rimborso, reclami della clientela).
Vettori	Agli offerenti che realizzano trasporti fisici come cosiddetti vettori (ad es. imprese dei tp o taxi) o che possiedono e mettono a disposizione un'infrastruttura o veicoli come gestori (ad es. Mobility) si uniscono sempre più spesso intermediari che non offrono direttamente mobilità, ma distribuiscono le offerte corrispondenti e in parte le combinano (ad es. Whim, moovel).

1 Ambito di validità

1.1 Panoramica grafica



Al centro della presente prescrizione vi sono tutti gli attori riportati in azzurro (o utenti NOVA) che scambiano dati tra NOVA («piattaforma») e i propri sistemi informativi (ad es. canali di distribuzione, punti vendita, dispositivi di controllo ecc.).

Altre definizioni: Gli **intermediari** vendono assortimenti NOVA in rappresentanza di una o più imprese di trasporto incaricata/e della fornitura di servizi. I **vettori** realizzano trasporti fisici. I **titolari della tariffa** sono l'istanza che esercita il controllo sulle tariffe. I **fornitori di servizi** erogano una prestazione. I **terzi** sono organizzazioni che aderiscono alla piattaforma NOVA e che ad esempio distribuiscono l'assortimento NOVA. Gli utenti NOVA possono anche assumere diversi ruoli.

1.2 Contatto

In caso di domande su questa prescrizione:

Alliance SwissPass
c/o ch-integral
Länggassstrasse 7
3012 Berna

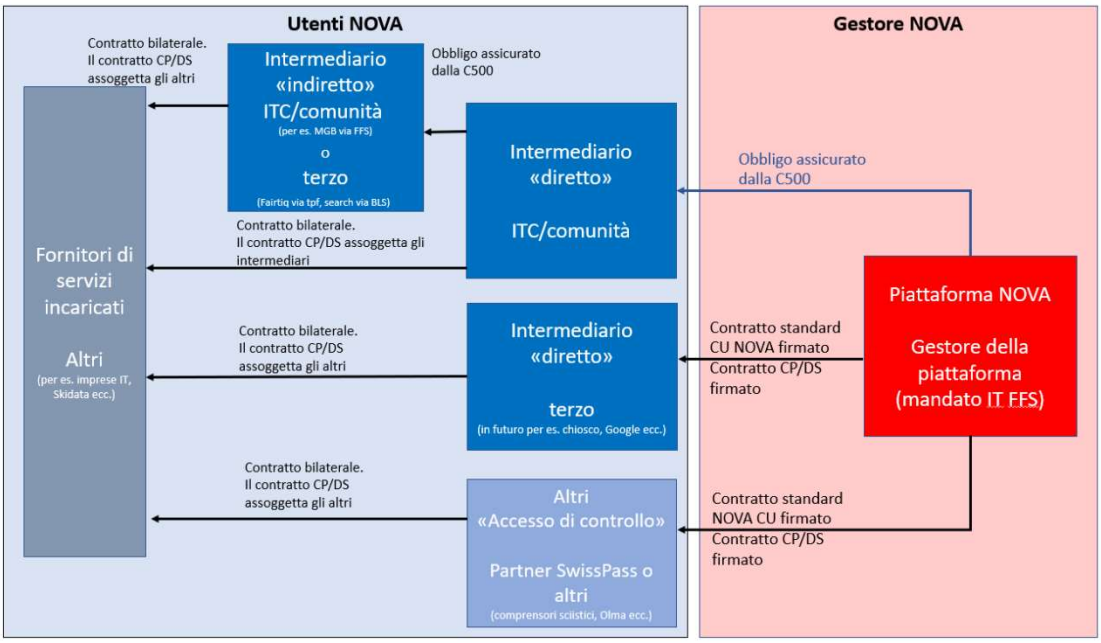
tarife@allianceswisspass.ch

2 Gestori del sistema interessati dalla presente prescrizione e relativi utenti

Tutte le persone che utilizzano la piattaforma NOVA vengono designate di seguito come «utenti NOVA», a prescindere dal fatto che partecipino direttamente o indirettamente alla piattaforma NOVA o che siano state incaricate di fornire un servizio.

2.1 Utenti della piattaforma NOVA

Per l'utilizzo della piattaforma NOVA sussistono le seguenti possibilità:



Accesso diretto per gli intermediari: gli intermediari soggetti alla C500 possono collegarsi direttamente alla piattaforma NOVA. Per loro vale il regolamento corrispondente.

Accesso diretto per i terzi: i terzi che desiderano distribuire servizi dei tp possono collegarsi direttamente alla piattaforma NOVA a condizione che firmino un «contratto standard CU NOVA» e il «contratto standard CP/DS». Con il «contratto standard CP/DS» i terzi si assumono l'obbligo di rispettare la presente P591.

Accesso diretto per i partner SwissPass/altri: i partner SwissPass o altri che utilizzano lo SwissPass per fornire i propri servizi (ad es. come vettori) possono identificare la propria clientela tramite SwissPass o utilizzare un accesso di controllo a condizione che firmino un «contratto standard CU NOVA» e il «contratto standard CP/DS». Con il «contratto standard CP/DS» i partner SwissPass/altri si assumono l'obbligo di rispettare la presente P591. Il gestore NOVA riceve una copia di questa convenzione.

Accesso indiretto per gli intermediari: indiretto significa che tramite l'accesso di un intermediario direttamente collegato, soggetto alla C500, possono collegarsi altri intermediari, anch'essi soggetti alla C500 (come ITC/comunità), nonché terzi, che

desiderano distribuire servizi dei tp. Ai partecipanti indiretti non è consentito concedere ad altre persone o imprese l'accesso per la distribuzione di servizi dei tp (nessun sotto-accesso). Per coloro che sono soggetti alla C500 vale la C500. I terzi hanno bisogno di un «contratto standard CU NOVA» e del «contratto standard CP/DS». Con il «contratto standard CP/DS» gli intermediari indiretti si assumono l'obbligo di rispettare la presente P591.

Fornitori di servizi incaricati: è possibile ricorrere a fornitori di servizi in qualsiasi momento, ma prima ne deve essere informato il gestore NOVA. I fornitori di servizi coinvolti sono persone ausiliarie ai sensi dell'articolo 101 CO. L'articolo 399 capoverso 2 CO è espressamente escluso. Gli utenti NOVA devono sottoscrivere una convenzione con il fornitore di servizi coinvolto, il quale si assume l'obbligo di rispettare la presente P591. Il gestore NOVA riceve una copia di questa convenzione. Con il «contratto standard CP/DS» i fornitori di servizi incaricati si assumono l'obbligo di rispettare la presente P591. Se i fornitori di servizi incaricati ricorrono ad altri subfornitori, per questi ultimi valgono gli stessi obblighi.

2.2 Gestore NOVA

È il mandatario incaricato dall'Alliance SwissPass e ha la sovranità per esercitare il controllo sugli standard minimi vincolanti per quanto riguarda i requisiti, l'attuazione e la sorveglianza delle prescrizioni tecniche in materia di CP/DS.

2.3 Processo di attivazione e accesso alla piattaforma NOVA

Con la firma del contratto per l'utilizzo della piattaforma NOVA, il contraente conferma di rispettare appieno le presenti prescrizioni P591.

3 Altre disposizioni

3.1 Disattivazione per motivi di sicurezza

In caso di incidente di sicurezza, il gestore NOVA può disattivare temporaneamente e immediatamente singoli canali o un utente NOVA. Il canale o l'utente NOVA sospeso sarà riattivato solo dopo che il gestore NOVA avrà accettato la prova della risoluzione del problema sulla base di un'analisi della causa radice. Le spese sostenute al riguardo saranno a carico degli utenti NOVA che hanno causato il problema.

3.2 Diritto di audit

Prima della messa in servizio e durante il periodo di utilizzo da parte di un utente (ad es. in caso di nuove release o dopo gli incidenti), il gestore NOVA ha il diritto di verificare il rispetto della presente prescrizione o di incaricare della verifica una società di audit indipendente. All'auditore devono essere concessi gli accessi, i diritti di accesso e le autorizzazioni nonché i supporti per effettuare l'audit. Se l'utente NOVA rifiuta l'accesso ai sistemi e ai documenti ai sensi di questa disposizione, il gestore NOVA sospende l'utilizzo di NOVA per la persona interessata.

Se l'auditore individua vulnerabilità, l'utente NOVA può essere obbligato a contribuire ai costi dell'audit. A partire da un risultato conforme al livello CVSS 7, il soggetto sottoposto ad audit si fa carico dei costi complessivi dell'audit.

3.3 Misure tecniche e organizzative

Le disposizioni e misure tecniche conformemente all'allegato alla P591 devono essere rispettate da tutti gli utenti NOVA.

3.4 Responsabilità e garanzia

L'Alliance SwissPass e il gestore NOVA non danno alcuna garanzia in merito alla disponibilità della piattaforma NOVA. Gli utenti NOVA prendono atto che la piattaforma può presentare restrizioni o addirittura non essere disponibile a causa di lavori di manutenzione, guasti tecnici o altre ragioni.
L'Alliance SwissPass e il gestore NOVA non si assumono alcuna responsabilità per danni indiretti, danni conseguenti, per lucro cessante, guadagni mancati, perdita di avviamento o mancati risparmi degli utenti NOVA.

Gli utenti NOVA prendono atto che i contratti con i loro clienti finali (consumatori) vengono conclusi direttamente tra questi e il vettore o l'offerente terzo. Il gestore NOVA e l'Alliance SwissPass non si assumono alcuna responsabilità derivante da questi contratti. Nel caso di una rivendicazione nei confronti del gestore NOVA o dell'Alliance SwissPass, gli utenti NOVA lo/la sollevano da tale responsabilità e si fanno carico anche dei costi derivanti dalla necessità di difendersi in sede giudiziaria.

Gli utenti NOVA direttamente collegati alla piattaforma NOVA sono responsabili del comportamento degli utenti NOVA indirettamente partecipanti da loro collegati.

Inoltre, tutti gli utenti NOVA rispondono del comportamento dei fornitori di servizi incaricati (ad es. subappaltatori, terzi coinvolti) come del proprio comportamento. Essi sono tenuti a stipulare un contratto di nomina a responsabile del trattamento con i fornitori di servizi incaricati.

3.5 Esclusione dall'utilizzo della piattaforma

Se un utente NOVA viola la presente prescrizione, il gestore NOVA fissa per iscritto un termine adeguato entro il quale l'utente deve correggere lo scostamento. Se una volta trascorso tale termine la violazione persiste, l'utente NOVA viene esortato a intervenire fissando un ultimo termine per la rettifica. Inoltre lo si avverte che, in caso di mancato rispetto di tale termine, potrà essere escluso dall'utilizzo della piattaforma NOVA.
Se un utente NOVA viola questa prescrizione più volte, potrà altresì escluso dall'utilizzo della piattaforma una volta avvertito dell'esclusione in caso di recidiva.

Il gestore NOVA si riserva il diritto di disattivare un utente NOVA in qualsiasi momento per motivi di sicurezza, ai sensi della cifra 3.1 di cui sopra.

3.6 Entrata in vigore e periodo transitorio

Con decisione della KoV dell'11 dicembre 2023, la prescrizione entra in vigore il 1º gennaio 2024. Per gli utenti NOVA già collegati è previsto un unico periodo transitorio di 12 mesi durante il quale, nei primi 6 mesi, deve essere dimostrata un'autovalutazione. Le eventuali vulnerabilità individuate devono essere documentate insieme alle misure corrispondenti o concretizzate nell'ambito di un piano di attuazione.