Policy NETTuno
in materia di protezione e disponibilità dei dati relativi ai servizi web

Premessa

Il presente documento descrive la policy NETTuno in materia di sicurezza delle informazioni, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web NETTuno.

NETTuno è impegnata costantemente nel migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, nell'ottica della salvaguardia dell'integrità e della riservatezza dei dati, della disponibilità dei servizi e delle informazioni in tempi adeguati e della continuità operativa dei servizi e dei sistemi. In questo contesto, NETTuno adotta tutti gli accorgimenti organizzativi, le soluzioni tecniche e procedurali idonee al mantenimento e ripristino delle condizioni di funzionamento e di operatività antecedenti ad eventuali eventi disastrosi ed è impegnata, con continuità, ad adottare tutte le misure di sicurezza che trovano fondamento e riferimento all'interno del quadro normativo italiano e europeo (Regolamento UE 2016/679, Linee guida AgID per il Disaster Recovery, Circolare AgID nr. 2/2017 sulle misure minime di sicurezza ICT per le PP.AA.) e dei più elevanti standard di sicurezza delle informazioni.

In qualità di fornitore di servizi SaaS, NETTuno è stata presente da Giugno 2019 fino a Gennaio 2023 nel catalogo AgID e da Febbraio 2023 è presente nel catalogo dei servizi Cloud per la PA qualificati di ACN.

Il Sistema di Gestione della Sicurezza delle Informazioni di NETTuno, nell'ambito dei servizi di progettazione, sviluppo, assistenza ed erogazione, in modalità cloud SaaS e on-premises, di software gestionale per le scuole di ogni ordine e grado e privati e di erogazione di servizi in modalità Cloud SaaS per la gestione di documenti digitali , è inoltre certificato secondo la norma UNI CEI EN ISO/IEC 27001:2022 [certificato n. 024G-NET-SI/17/18 Si Cert Italy S.r.l.] e con i controlli previsti dalle linee guida ISO/IEC 27017:2021 e ISO/IEC 27018:2020.

Tipologia dei dati e delle informazioni gestiti dalla NETTuno

I dati gestiti da NETTuno consistono nelle informazioni (generiche e personali) contenute negli archivi e/o nei documenti delle scuole e dei clienti fruitori dei medesimi servizi e nei profili degli utenti fruitori dei servizi web NETTuno.

In riferimento alle informazioni contenute negli archivi, la natura dei dati e dei documenti varia in base alle caratteristiche del servizio attivato da ogni singola istituzione scolastica o cliente. Possono quindi essere conservate informazioni personali e, nel caso di servizi collegati alla gestione del personale e degli alunni, anche dati appartenenti alle categorie particolari di cui agli artt. 9 e 10 del Regolamento UE 2016/679 [specificamente quelle riepilogate nelle schede allegate al D.M. 305/2006, recante identificazione degli ex dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione].

I dati ed i documenti sono conservati all'interno dei database degli applicativi secondo la logica di raccolta e standardizzazione del singolo software ed etichettati secondo la classificazione delle informazioni del sistema di gestione.

I documenti sono raccolti e archiviati in appositi repository, secondo la logica di classificazione delle informazioni impostata dal cliente.

Modello di responsabilità condivisa (shared responsibility)

NETTuno lavora in qualità di fornitore di servizi in Cloud mettendo a disposizione applicativi in modalità SaaS e erogando i relativi servizi di assistenza e manutenzione. Si avvale di fornitori di servizi cloud qualificati e certificati secondo la vigente normativa ed identifica nei propri contratti gli specifici ruoli attribuiti a ciascun fornitore del servizio.

Per rappresentare in maniera completa la distribuzione dei ruoli e rendere gli utilizzatori dei servizi consapevoli delle loro responsabilità nell'uso del servizio cloud, NETTuno ha elaborato il seguente modello di responsabilità condivisa. Nello schema, è messo in evidenza, per ogni tipo di dato o dispositivo, il responsabile della sicurezza dei dati.

Responsabilità	**Cliente** ✅	**Condivisa** 🤝	**NETTuno** ☁️
Information & Data	✅		
Dispositivi (PC, Mobile)	✅		

Responsabilità	Cliente ✅	Condivisa 🤝	NETTuno ☁️
Accounts & Identities	✅		
Identity & Directory Infrastructure		🤝	
Applications		🤝	
Network Controls		🤝	
Operating System		🤝	
Physical Hosts			☁️
Physical Network			☁️
Physical Datacenter			☁️

Architettura del sistema informatico

I database server, i repository di documenti e le relative copie di backup sono ospitati presso la piattaforma cloud AWS (Amazon Web Services) messa a disposizione dal Cloud Service Provider AWS EMEA sarl, società di diritto europeo, all'interno di data center localizzati nel territorio della Unione Europea. AWS ha stipulato con NETTuno accordi contrattuali conformi alla vigente normativa e adottato misure di sicurezza che impediscono ogni accesso ai dati da soggetti fuori dallo Spazio Economico Europeo (tramite la cifratura degli storage e dei dati – con chiave di cifratura disponibile alla sola NETTuno - e il blocco degli accessi remoti).

Il Cloud AWS è strutturato in "regioni", costituite da più "zone di disponibilità" (AZ), ognuna delle quali è una partizione completamente isolata dell'infrastruttura AWS, costituita da data center provvisti di alimentazione, rete e connettività ridondanti, ognuno nella propria struttura separata. Per i dati dei propri clienti, NETTuno ha scelto la regione Europa Irlanda, situata nella Repubblica d'Irlanda, composta da 3 zone di disponibilità e la regione Europa Milano, anch'essa composta da 3 zone di disponibilità. Con la loro infrastruttura di alimentazione, le zone di disponibilità sono fisicamente separate tra loro da una distanza significativa di molti chilometri.

I database sono conservati su server dedicati Aruba .

I file dei documenti sono conservati negli storage (contenitori) di Amazon S3.

I backup di database e file sono conservati negli storage di Amazon S3.

L'amministrazione dei servizi di gestione delle applicazioni e dei database è affidata esclusivamente a personale interno a NETTuno.

Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.

L'accesso ai servizi di amministrazione è eseguito attraverso utenze di dominio nominative adottando il meccanismo di autenticazione forte a due fattori secondo un approccio basato sull'analisi dei rischi.

Con periodicità infrannuale, sulla base del piano degli audit interni, viene eseguito il monitoraggio sui log degli accessi degli amministratori di sistema da parte del personale all'uopo designato (auditor incaricato o responsabile del SGSI).

I log degli accessi eseguiti dagli amministratori di sistema sono archiviati per un periodo minimo di 18 mesi.

Modalità di gestione dei dati e di erogazione del servizio

Tutti i dati ed i backup archiviati in Amazon S3 sono protetti con la crittografia, mediante l'Advanced Encryption Standard AES-256. Le applicazioni ed i database risiedono su server dedicati ad alte prestazioni in hosting su provider Aruba, con dischi ridondati, preservando così i clienti da rischi di interruzione prolungata dei servizi e/o di perdita delle informazioni. Le macchine sono costantemente monitorate e la scalabilità viene effettuata manualmente, qualora ce ne fosse bisogno, in base agli indicatori di monitoraggio.

Backup e ripristino dei dati, garanzie di continuità operativa

Per ogni istanza di database, viene creata e mantenuta una copia di backup giornaliera per 30 giorni (periodo di retention dei backup). La creazione dei backup non provoca alcuna interruzione delle operazioni di scrittura e lettura.

Durante questo periodo, è possibile eseguire il ripristino di una istanza di database a un punto temporale specifico.

Decorso questo periodo, viene mantenuta una copia settimanale per ulteriori 335 giorni. Successivamente viene mantenuta una copia mensile per minimo ulteriori 365 giorni.

Per offrire un pari livello di protezione anche ai documenti, NETTuno ha attivato la funzione *Versioning* che consente di recuperare e ripristinare qualsiasi versione di ogni file di documento memorizzato nello storage Amazon S3.

Il servizio di AWS garantisce una durabilità dei dati pari ad oltre il 99,9% perché crea e mantiene automaticamente copie di tutti gli oggetti su più sistemi.

Per tutelare i propri clienti, NETTuno ha messo in funzione un piano di continuità operativa molto dettagliato, che mira a garantire il ripristino di tutte le informazioni contenute nelle repliche anche in caso di disastro, secondo i seguenti SLA:

- RTO: il tempo massimo di recupero e ripristino delle informazioni è fissato in 12 ore dall'incidente.
- RPO: il punto massimo di perdita di dati in caso di incidente è 24 ore (per via del backup giornaliero, se l'incidente avviene prima della copia, il massimo di dati persi è fino all'ultima esecuzione del backup del giorno precedente).

I due SLA, combinati, mirano a garantire ai clienti dei servizi cloud che in caso di disastro, NETTuno sarà in grado di ripristinare la disponibilità di tutti i dati, fatti salvi quelli registrati nelle ultime 24 ore, in un massimo di 12 ore.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web NETTuno, attraverso le funzionalità degli applicativi stessi, è di esclusiva pertinenza della scuola.

In fase di attivazione di una nuova utenza, viene richiesta l'indicazione di un'indirizzo mail, necessaria se si desidera eseguire il reset password dell'utenza.

L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente dagli applicativi NETTuno, accedendo alla gestione "Modifica Profilo".

Accesso ai servizi web

L'accesso ai servizi può essere effettuato, oltre che tramite le credenziali fornite dalla scuola, anche mediante SPID di livello 2 (se l'utente è stato abilitato dal gestore delle utenze della scuola e qualora la scuola abbia sottoscritto l'accordo di servizio per la registrazione in AgID).

Ai fini della protezione e della conservazione delle password degli utenti dei servizi web, NETTuno ha adottato un algoritmo di password hashing raccomandato nelle specifiche "Linee guida funzioni crittografiche" che nel dicembre 2023 l'Agenzia per la Cybersicurezza Nazionale (ACN) e il Garante per la protezione dei dati personali hanno messo a punto.

Tracciamento dei log nei servizi web

Ai fini della sicurezza, NETTuno esegue il tracciamento degli "*accessi*" agli applicativi web NETTUno e – per le applicazioni più critiche – delle "*operazioni*" effettuate dagli utenti all'interno degli stessi.

In considerazione del volume e della eterogeneità dei log raccolti, che possono perdere di efficacia informativa se generalizzati tra applicativi, vengono raccolte e conservate tutte e sole le informazioni utili in ogni applicativo, nel rispetto del principio di minimizzazione.

Alla data di aggiornamento di questa policy, sono disponibili e possono essere richiesti secondo la procedura che segue:

- i log degli accessi agli applicativi, per tutti gli utenti, effettuati nell'arco degli ultimi 24 mesi mobili;
- i log delle operazioni significative sui database, intesi come le query SQL lanciate sulle banche dati degli applicativi web (es. inserimento, modifica, cancellazione) effettuati nell'arco degli ultimi 24 mesi mobili, al fine di analisi di bug di sistema o di segnalazioni che richiedono l'analisi di eventuali incidenti;
- i log essenziali di ulteriori operazioni significative, variabili in base all'applicativo, qualora ritenuti rilevanti per verifiche ulteriori rispetto a bug, incidenti, data breach, per un massimo di 24 mesi mobili.

Per le eventuali richieste dei log da parte dei clienti, la richiesta deve provenire da casella PEC ufficiale del cliente, da inviare tramite PEC all'indirizzo nettuno-srl@pec.it. La richiesta di log deve essere sottoscritta dal Dirigente Scolastico, circostanziata e motivata.

Un eventuale prolungamento dei tempi di conservazione può aver luogo in relazione:

- a particolari esigenze tecniche o di sicurezza;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Oltre ai suddetti dati, i sistemi informatici e le procedure software preposte al funzionamento dei servizi NETTuno acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati e che vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso delle applicazioni e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione.

Procedure di verifica del sistema di protezione dei dati

Con cadenza annuale vengono svolte da società terze, specializzate nel settore della sicurezza informatica, Penetration test e verifiche di Vulnerability Assessment.

Per quanto riguarda l'aggiornamento delle misure di sicurezza, i server ricevono continuamente aggiornamenti automatici. NETTuno è inoltre iscritta a servizi informativi, per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione dei Data Center e Cloud Service Provider

NETTuno si affida esclusivamente a Data Center e CSP di comprovata affidabilità ed esperienza in materia di sicurezza informatica, e comunque previa verifica delle misure fisiche, logiche e organizzative poste in capo alle infrastrutture informatiche fornite.

Ad ogni fornitore è richiesta come requisito la certificazione ISO 27001, 99% la qualificazione come CSP presso AgID, uno SLA di connettività di almeno il su base annua ed una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.

Modalità di trasmissione dei dati

I dati viaggiano sulla rete criptati, secondo il protocollo SSL che garantisce il massimo livello di sicurezza a protezione delle trasmissioni telematiche.

Disponibilità dei dati

Per gli applicativi web NETTuno durante la vigenza del contratto è possibile richiedere in qualsiasi momento una copia in locale dei dati residenti presso i server NETTuno.

La procedura è integrata e disponibile nella Suite Segreteria Digitale di NETTuno, nell'area **Backup → Richiedi copia di tutti i dati,** e consente di richiedere una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola, nella persona del Dirigente scolastico o di un suo delegato.
Per la restituzione dei dati degli applicativi web non presenti nell'elenco della procedura prima descritta e per tutti quelli on premise, la richiesta deve essere inoltrata tramite PEC all'indirizzo nettuno-srl@pec.it.

I dati contenuti nei database e nei repository delle applicazioni per le quali è stata richiesta l'esportazione vengono forniti in formato aperto, con tracciato definito da NETTuno. In caso di richiesta tramite la Suite Segreteria Digitale, sono scaricabili dalla medesima area; in caso di richiesta tramite PEC, vengono resi disponibili mediante apposito link comunicato con la stessa PEC.
In entrambi i casi, il download rimane disponibile per 30 giorni solari dalla messa a disposizione dei dati. Decorso tale termine, la disponibilità per il download viene disattivata.

Scadenza e risoluzione dei contratti, restituzione, cancellazione e fruibilità dei dati

In caso di cessazione del contratto di licenza SaaS relativo a un servizio web NETTuno, la scuola – su richiesta del Dirigente scolastico – può optare per:

- la restituzione e cancellazione/anonimizzazione dei dati;
- la restituzione e mantenimento dei dati, a fronte del pagamento di un canone.

Il Cliente dispone di 30 giorni solari dalla data di cessazione del contratto per richiedere l'esportazione dei propri dati, secondo le modalità sopra descritte nel paragrafo "Disponibilità dei dati".

I dati e i documenti richiesti vengono restituiti in formato aperto, nei tempi tecnici necessari all'esportazione e mediante modalità di trasmissione sicure. Una volta messi a disposizione, restano disponibili per il download per 30 giorni solari, secondo quanto previsto nel paragrafo "Disponibilità dei dati".

I tempi tecnici occorrenti alla successiva cancellazione dei dati possono variare da 2 mesi a 12 mesi, più i tempi di retention del backup sopra indicati (30 + 335 gg + 365 gg = 2 anni / 24 mesi), a seconda della natura delle informazioni coinvolte e delle applicazioni interessate. Il periodo è peraltro funzionale ad eventuali verifiche da parte del cliente sull'operazione di migrazione dati eseguita dal nuovo fornitore. Il tempo massimo di conservazione dei dati contenuti nei database dopo la cessazione del contratto e/o la richiesta di cancellazione dei dati è 12+2 mesi. Parimenti, il tempo massimo di conservazione dei documenti contenuti nei repository dopo la cessazione del contratto e/o la richiesta di cancellazione dei dati è 12+2 mesi, al termine dei quali la NETTuno procederà alla cancellazione logica dei files dai sistemi. L'attivazione del versioning nei repository richiede però ulteriori 30 gg perché la cancellazione dei files sia effettiva. Alla cessazione del contratto per qualsivoglia ragione, NETTuno non ha più alcun titolo per poter trattare i dati e documenti mantenuti per conto del cliente; pertanto, dovrà necessariamente procedere alla procedura di chiusura degli accessi e cancellazione dei dati sopra descritta.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito NETTuno (www.nettunopa.it) all'interno della sezione "Policy e Documenti" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity di NETTuno e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione a tutte le scuole clienti mediante email o avviso sul sito web e/o applicativi NETTuno.

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1.0	02.01.2025	Policy NETTuno in materia di protezione e disponibilità dei dati relativi ai servizi web	Daniele Rapillo	Davide Dossena
1.1	07.10.2026	Allineamento della Policy alle Condizioni generali di licenza v.1.4: revisione delle modalità di esportazione e disponibilità dei dati alla scadenza del contratto.	Daniele Rapillo	Davide Dossena