



SICUREZZA DELLE
INFORMAZIONI – CONTROLLI
ISO 27017 | 27018

SICUREZZA DELLE INFORMAZIONI – CONTROLLI ISO 27017 | 27018

Data Creazione Documento	10 gennaio 2025
Data Aggiornamento Documento	10 gennaio 2025
Revisione Documento	00
Autore	Responsabile Sicurezza Informazioni
Approvato da	Direzione
Classificazione	Pubblico

Campo applicazione		
<i>Progettazione, sviluppo, installazione e assistenza post vendita di prodotti software erogati in modalità SaaS.</i>		
SEDI	Via Camarele, 13 – Frazione: Arbizzano – Negrar di Valpolicella (VR)	
Esclusioni		
SEDI	Nessuna	
ATTIVITÀ	Nessuna	
PRODOTTI / SERVIZI	Nessuno	

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



Premessa

Il presente documento, redatto e aggiornato da AT Service Srl, ha lo scopo di informare il proprio cliente circa i controlli applicati all'interno della propria infrastruttura Cloud

DEFINIZIONI

DEFINIZIONE/ACRONIMO	DESCRIZIONE
Data Center	Infrastruttura di AT Service presso un provider
Cloud	Data Center o Cloud di AT Service o dei propri partner
AT Service	Per brevità si intende AT Service Srl
Prodotto/Soluzione/Servizio SaaS	Sono i software sviluppati da AT Service offerti ai propri clienti in modalità SaaS, come Dedalo.top
Dedalo / Dedalo.top	Software SaaS fornito da AT Service Srl ai propri clienti per la gestione dei servizi scolastici e in uso alle amministrazioni comunali per la gestione, nonché ai genitori degli alunni per le interazioni necessarie (es: pagamenti, richieste, ecc.)

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



CONTROLLI NORMA UNI CEI EN ISO/IEC 27017:2021

NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE																
5.1.1	Policies for information security	Politiche del Sistema di Gestione della Sicurezza delle Informazioni: AT Service ha definito la propria Politica di sicurezza delle Informazioni aggiornata periodicamente e pubblicata sul proprio sito web.	https://www.at-service.it/certificazioni.asp																
6.1.1	Information security roles and responsibilities	<p>Ruoli e responsabilità: All'interno dell'ambito di responsabilità di AT Service come fornitore di soluzioni SaaS, AT Service ha definito le figure, i ruoli, le competenze e le responsabilità connesse ai processi, secondo i principi di segregation of duties, least privilege e dual control.</p> <p>Segregation of Duties (SoD) - Nell'ambito dei processi operativi dei servizi, una sequenza di procedure viene svolta da diverse persone, mai una sola, a garanzia che il controllo dell'intero processo non sia affidato ad un singolo individuo.</p> <p>Least privilege - I permessi di accesso a locali, apparati, dati, funzionalità, ecc. sono concessi, al personale addetto ai servizi, secondo il principio del "least privilege" ossia nella misura necessaria affinché tali risorse possano svolgere i compiti loro assegnati, ma non oltre.</p> <p>Dual control - Le procedure più critiche dal punto di vista della sicurezza prevedono il concorso di almeno due persone.</p>	<p>Tabella responsabilità per tutti i Prodotti SaaS di AT Service</p> <table border="1"> <thead> <tr> <th>Ambito</th> <th>Responsabile</th> </tr> </thead> <tbody> <tr> <td>Data</td> <td>Cliente</td> </tr> <tr> <td>Application</td> <td>AT Service</td> </tr> <tr> <td>System</td> <td>AT Service</td> </tr> <tr> <td>Servers</td> <td>AT Service</td> </tr> <tr> <td>Storage</td> <td>AT Service</td> </tr> <tr> <td>Network</td> <td>AT Service</td> </tr> <tr> <td>Physical</td> <td>Aruba</td> </tr> </tbody> </table> <p>Indirizzo mail dedicato all'assistenza assistenza@at-service.it</p>	Ambito	Responsabile	Data	Cliente	Application	AT Service	System	AT Service	Servers	AT Service	Storage	AT Service	Network	AT Service	Physical	Aruba
Ambito	Responsabile																		
Data	Cliente																		
Application	AT Service																		
System	AT Service																		
Servers	AT Service																		
Storage	AT Service																		
Network	AT Service																		
Physical	Aruba																		
6.1.3	Contact with authorities	Contatti con le autorità: AT Service è in contatto costante con le autorità competenti la materia di sicurezza delle informazioni e protezione dei dati. GARANTE PRIVACY ACN	AT Service ha nominato un DPO raggiungibile tramite mail: info@at-service.it o telefono al 045.7513353																
7.2.2	Information security awareness, education and training	<p>Formazione del personale: il personale di AT Service e i sub-appaltatori addetti al servizio hanno adeguata competenza ed esperienza, e viene loro fornito o richiesto un addestramento specifico a fronte di ogni importante aggiornamento dei sistemi.</p> <p>Consapevolezza (Awareness): periodicamente, il personale di AT Service viene sensibilizzato sulle tematiche di sicurezza, sul cybercrime in generale e sulle best practice da adottare, mediante specifici corsi di formazione. Ai sub-appaltatori viene richiesto quale requisito essenziale per poter collaborare con AT Service.</p> <p>Non Disclosure Agreement (NDA): ai nuovi assunti e ai sub-appaltatori viene richiesto di sottoscrivere un accordo di confidenzialità al fine di tutelare il know-how aziendale e le informazioni trattate nell'ambito della collaborazione.</p>																	
8.1.1	Inventory of assets	<p>Inventario Asset: all'interno di AT Service è presente un inventario aggiornato degli asset, al cui interno è censita l'infrastruttura fisica e virtuale e la loro collocazione.</p> <p>AT Service testa e censisce l'hardware e il software autorizzato all'inserimento nell'infrastruttura</p>																	

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE
		aggiornato l'inventario al termine delle nuove installazioni. Ogni asset è classificato per tipologia di informazioni trattate e caratteristiche tecniche, nonché relativi responsabili.	
8.2.2	Labelling of information	Etichettatura delle informazioni: AT Service adotta un sistema per etichettare le informazioni in base alla classificazione definita nelle proprie procedure.	I Prodotti SaaS offerti da AT Service non prevedono per il Cliente la possibilità di classificare o etichettare le informazioni e le risorse associate.
9.1.2	Access to networks and network services	Controlli di accesso: il personale di AT Service che accede alle risorse è stato autorizzato. Prima di accedere ai sistemi interni, viene chiesto al personale che ne ha diritto di identificarsi e di autenticarsi (tramite nome utente, password). Il personale AT Service può accedere, previa autenticazione, alle sole risorse per cui è stato autorizzato.	
9.2.1	User registration and deregistration	Alla fornitura di un servizio, AT Service crea le utenze necessarie all'utilizzo di Dedalo, le cui password sono modificabili in autonomia dall'utente.	Il Cliente può utilizzare il sistema di autenticazione nativo del prodotto AT Service. Gli utilizzatori finali del prodotto accedono ai servizi tramite SPID.
9.2.2	User access provisioning	Ogni Prodotto SaaS di AT Service prevede la gestione degli accessi, tra cui le funzioni di registrazione e annullamento	
9.2.3	Management of privileged access rights	Gestione dei privilegi di accesso: i Prodotti SaaS di AT Service gestiscono due tipologie di accesso. Per i Clienti (ovvero gli Enti Locali) il sistema proprietario del prodotto si basa su username e password. La seconda per gli utilizzatori tramite SPID.	
9.2.4	Management of secret authentication information of users	Password policy - Coerentemente con le policy di sicurezza di AT Service e nel rispetto della normativa vigente, è applicata una politica sicura di gestione delle password.	Al Cliente vengono fornite istruzioni dirette o tramite il manuale di prodotto.
9.4.4	Use of privileged utility programs	Utilizzo di programmi di utilità privilegiati: in conformità alle policy della norma ISO 27001, AT Service ha definito una politica di uso dei programmi di utilità privilegiata, autorizzato gli utenti abilitati, definendo e censendo i programmi autorizzati.	
10.1.1	Policy on the use of cryptographic controls	Canale sicuro SSL - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).	
10.1.2	Key management	Le chiavi crittografiche eventualmente utilizzate da AT Service sono conservate all'interno del Cloud. Policy: AT Service ha definito internamente una politica per l'uso della crittografia.	
11.2.7	Secure disposal or reuse of equipment	Alla conclusione del contratto di un Prodotto SaaS, AT Service provvede alla cancellazione e rimozione definitiva	

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE
		dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo PEC. AT Service gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.	
12.1.2	Change management	I cambiamenti resi necessari dalle circostanze tecniche e di gestione vengono gestiti in modo controllato per permettere di verificarne i risultati e di mantenere traccia delle attività svolte.	Per le attività impattanti sul servizio AT Service informa i propri clienti mediante comunicazioni mail preventive.
12.1.3	Capacity management	Al fine di garantire la corretta erogazione del servizio, AT Service monitora costantemente il proprio Cloud e tutte le risorse di cui dispone, analizzando le capacità e adottando gli opportuni accorgimenti per lo sfruttamento ottimale delle stesse e per assicurare la normale fruizione dei Prodotti SaaS.	
12.3.1	Information backup	Backup delle informazioni: la struttura dei backup, i controlli, la verifica, i test, sono a carico di AT Service che garantisce al Cliente la conservazione di un backup: <ul style="list-style-type: none"> - Degli ultimi 60 giorni - Di un backup al mese per 12 mesi Inoltre, le componenti funzionali all'erogazione dei servizi di AT Service, la gestione degli utenti e le altre componenti architettoniche seguono le procedure di backup definite a livello aziendale e vengono periodicamente verificate e testate. I sistemi di backup prevedono sistemi di notifica in caso di problemi.	Il Cliente non dispone dei backup eseguiti da AT Service, ma ne può richiedere copia ad AT Service in qualsiasi momento.
12.4.1	Event logging	Log applicazioni: la soluzione SaaS Dedalo, prodotta da AT Service, dispone di un proprio Log.	
12.4.3	Administrator and operator logs	Log applicazioni: la soluzione SaaS Dedalo, prodotta da AT Service, dispone di un proprio Log.	
12.4.4	Clock synchronization	Sincronizzazione – AT Service utilizza il sistema NTP per sincronizzare gli orologi dei propri asset fisici e virtuali e mantenere coerenza degli eventi. La fonte per la sincronizzazione dell'orologio è time.windows.com.	
12.6.1	Administrator and operator logs	Processo di Vulnerability Management – Il perimetro AT Service, composto dal Cloud e i prodotti SaaS, viene regolarmente scansionato da strumenti automatici e da professionisti qualificati del settore al fine di identificare ogni possibile vulnerabilità anche solo potenziale. Le criticità individuate vengono segnalate al responsabile competente, dando il via al ciclo di risoluzione della problematica che può concludersi con un nuovo rilascio oppure con una mitigazione. Per verificarne l'efficacia, si esegue infine una nuova scansione per avere la certezza del rientro della vulnerabilità.	Il Cliente può segnalare eventuali Vulnerabilità riscontrate tramite mail all'indirizzo info@at-service.it
13.1.3	Segregation in network	AT Service, in conformità con gli standard di sicurezza internazionali, garantisce la segregazione dell'accesso dei Clienti rispetto agli accessi interni degli operatori di AT Service. Inoltre, AT Service assicura un'efficace separazione degli ambienti in configurazione multi-tenant, a tutela della riservatezza e dell'integrità dei dati di ciascun Cliente.	

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE
14.1.1	Information security requirements analysis and specification	AT Service informa i propri Clienti mediante il presente documento e la pagina "PRIVACY CERTIFICAZIONI E SICUREZZA" presente e aggiornata sul proprio sito web	https://www.at-service.it/certificazioni.asp
14.2.1	Secure development policy	AT Service adotta le Linee Guida AGID e la metodologia OWASP come riferimenti fondamentali per lo sviluppo dei propri prodotti, garantendo così standard elevati di qualità e sicurezza.	
15.1.1	Secure development policy	Il Cloud AT Service è locato in Italia presso un'infrastruttura di cloud computing avanzata che fornisce servizi scalabili, sicuri e distribuiti a livello nazionale, e ridondati per garantirne la disponibilità.	
15.1.2	Addressing security within supplier agreements	Le soluzioni SaaS di AT Service prevedono l'accettazione delle condizioni contrattuali al cui interno sono specificate le responsabilità di AT Service e del Cliente.	
15.1.3	Information and communication technology supply chain	Il Cloud AT Service è locato in Italia presso un'infrastruttura di cloud computing avanzata che fornisce servizi scalabili, sicuri e distribuiti a livello nazionale, e ridondati per garantirne la disponibilità.	
16.1.1	Responsibilities and procedures	Le soluzioni SaaS di AT Service prevedono l'accettazione delle condizioni contrattuali al cui interno sono specificate le responsabilità di AT Service e del Cliente.	Il Cliente può segnalare eventuali Incidenti di Sicurezza tramite mail all'indirizzo info@at-service.it In caso di Data Breach, Il Cliente può contattare il DPO designato da AT Service scrivendo una e-mail all'indirizzo info@at-service.it o contattando il numero 045.7513353
16.1.2	Reporting information security events	AT Service mette a disposizione un indirizzo mail, oltre al numero telefonico, tramite cui aprire segnalazioni per qualsiasi problematica o richiesta.	Il Cliente può segnalare eventi di sicurezza tramite mail all'indirizzo info@at-service.it
16.1.7	Collection of evidence	AT Service collaborerà con il Cliente per rispondere ad eventuali richieste di evidenze e/o prove da parte delle autorità fornendo all'occorrenza log o altre tipologie di evidenze	
18.1.1	Identification of applicable legislation and contractual requirements	Legge Italiana, Diritto d'autore, GDPR e Codice Privacy e Provvedimenti del Garante, Norme ISO 9001 27001 27017 27018	
18.1.2	Intellectual property rights	La proprietà intellettuale dei prodotti AT Service è soggetta al diritto d'autore italiano ed è di AT Service Srl.	Il Cliente può segnalare eventi reclami sulla proprietà intellettuale tramite mail all'indirizzo info@at-service.it
18.1.3	Protection of records	AT Service fornisce indicazioni sulla protezione dei dati tramite informativa privacy e nomina a Responsabile del	https://www.at-service.it/privacy/informativa_privacy.pdf

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE
		trattamento firmato nella fase di definizione contrattuale.	
18.1.5	Regulation of cryptographic controls	<p>Canale sicuro SSL - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione.</p> <p>Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).</p>	
18.2.1	Independent review of information security	AT Service sottopone i propri sistemi e relativi sistemi di gestione ad audit periodici effettuati da Enti di Certificazione. Queste informazioni possono essere richieste dal Cliente in casi di necessità.	
CLD 6.3.1	Shared roles and responsibilities within a cloud computing environment	AT Service è responsabile della sicurezza del proprio Cloud e dei propri prodotti SaaS.	
CLD 8.1.5	Removal of cloud service customer assets Control	<p>Alla conclusione del contratto di un Prodotto SaaS, AT Service provvede alla cancellazione e rimozione definitiva dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo PEC.</p> <p>AT Service gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.</p>	
CLD 9.5.1	Segregation in virtual computing environments	AT Service, in conformità con gli standard di sicurezza internazionali, garantisce la segregazione dell'accesso dei Clienti rispetto agli accessi interni degli operatori di AT Service. Inoltre, AT Service assicura un'efficace separazione degli ambienti in configurazione multi-tenant, a tutela della riservatezza e dell'integrità dei dati di ciascun Cliente.	
CLD 9.5.2	Virtual machine hardening	AT Service, in conformità agli standard internazionali di sicurezza, adotta procedure collaudate per la configurazione di ogni nuovo ambiente, fisico o virtuale, o nuovo servizio.	
CLD 12.1.5	Administrator's operational security	AT Service programma le attività critiche sui propri sistemi, comunicando preventivamente tramite mail ai propri clienti.	
CLD 12.4.5	Monitoring of Cloud Services	AT Service monitora i propri servizi informando i clienti su eventi rilevanti che possano compromettere o possano aver compromesso il servizio.	All'interno di Dedalo.top è presente una sezione di avvisi con cui AT Service comunica eventuali disservizi agli utilizzatori
CLD 13.1.4	Alignment of security management for virtual and physical networks	AT Service ha definito le politiche di configurazione delle reti fisiche e virtuali.	

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



CONTROLLI NORMA UNI CEI EN ISO/IEC 27018:2020

NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE
5.1.1	Policies for information security	Politiche del Sistema di Gestione della Sicurezza delle Informazioni: AT Service ha definito la propria Politica di sicurezza delle Informazioni aggiornata periodicamente e pubblicata sul proprio sito web	Politica Sicurezza Informazioni disponibile a link https://www.at-service.it/certificazioni.asp
6.1.1	Information security roles and responsibilities	AT Service ha nominato un DPO raggiungibile tramite mail: info@at-service.it o telefono al 045.7513353	Mail DPO info@at-service.it o telefono al 045.7513353
7.2.2	Information security awareness, education and training	Formazione del personale: il personale di AT Service e i sub-appaltatori addetti al servizio hanno adeguata competenza ed esperienza, e viene loro fornito o richiesto un addestramento specifico a fronte di ogni importante aggiornamento dei sistemi. Consapevolezza (Awareness): periodicamente, il personale di AT Service viene sensibilizzato sulle tematiche di sicurezza, sul cybercrime in generale e sulle best practice da adottare, mediante specifici corsi di formazione. Ai sub-appaltatori viene richiesto quale requisito essenziale per poter collaborare con AT Service. Non Disclosure Agreement (NDA): ai nuovi assunti e ai sub-appaltatori viene richiesto di sottoscrivere un accordo di confidenzialità al fine di tutelare il know-how aziendale e le informazioni trattate nell'ambito della collaborazione.	
9.2	User access management	Alla fornitura di un servizio, AT Service crea le utenze necessarie all'utilizzo di Dedalo, le cui password sono modificabili in autonomia dall'utente.	
9.2.1	User registration and de-registration	Alla fornitura di un servizio, AT Service crea le utenze necessarie all'utilizzo di Dedalo, le cui password sono modificabili in autonomia dall'utente.	
9.4.2	Secure log-on procedures	L'accesso al servizio Dedalo avviene tramite credenziali di accesso o sistema di autenticazione SPID	
10.1.1	Policy on the use of cryptographic controls	Canale sicuro SSL - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).	
11.2.7	Secure disposal or re-use of equipment	Alla conclusione del contratto di un Prodotto SaaS, AT Service provvede alla cancellazione e rimozione definitiva dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo PEC. AT Service gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.	
12.1.4	Separation of development, testing and operational environments	Eventuali test necessari, effettuati da AT Service avvengono esclusivamente nel perimetro AT Service, in appositi sistemi dedicati per garantire la protezione dei dati personali e delle informazioni.	
12.3.1	Information backup	Backup delle informazioni: la struttura dei backup, i controlli, la verifica, i test, sono a carico di AT Service	

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



		<p>che garantisce al Cliente la conservazione di un backup:</p> <ul style="list-style-type: none"> - Degli ultimi 60 giorni - Di un backup al mese per 12 mesi <p>Inoltre, le componenti funzionali all'erogazione dei servizi di AT Service, la gestione degli utenti e le altre componenti architetturali seguono le procedure di backup definite a livello aziendale e vengono periodicamente verificate e testate.</p> <p>I sistemi di backup prevedono sistemi di notifica in caso di problemi.</p>	
12.4.1	Event logging	Log applicazioni: la soluzione SaaS Dedalo, prodotta da AT Service, dispone di un proprio Log.	
12.4.2	Protection of log information	AT Service attua tutte le misure di sicurezza necessarie per la protezione delle informazioni di Log contenenti dati personali.	
13.2.1	Information transfer policies and procedures	AT Service ha definito una politica di trasferimento delle informazioni tramite canali di comunicazione sicuri.	
16.1	Management of information security incidents and improvements	AT Service coopererà con il Cliente nel caso di segnalazioni di incidenti di sicurezza delle informazioni, implementando controlli e apportando con rapidità i miglioramenti necessari affinché non riaccadano.	Il Cliente è responsabile dei dati personali contenuti nei prodotti SaaS AT Service
16.1.1	Responsibilities and procedures	AT Service ha definito le procedure per la gestione degli incidenti di sicurezza, con eventuale registrazione del Data Breach e relativa notifica al Garante e agli interessati (se previsto). A seguito di ogni incidente AT Service adotta procedure di miglioramento atte a evitare incidenti successivi.	
18.2.1	Independent review of information security	AT Service è certificata secondo lo schema della norma ISO UNI CEI EN ISO/IEC 27001:2024 con l'estensione dei controlli delle norme ISO UNI CEI EN ISO/IEC 27017 e 27018 ed è sottoposta periodicamente ad Audit di verifica da parte dell'Ente di Certificazione	Certificazioni AT Service disponibili al link https://www.at-service.it/certificazioni.asp
A.2.1	Obligation to co-operate regarding PII principals' rights	AT Service rende disponibile ai propri clienti l'informativa privacy e relativo modello di esercizio dei diritti dell'interessato. Ha inoltre nominato un DPO contattabile all'indirizzo info@at-service.it	Informativa privacy disponibile al link https://www.at-service.it/privacy/ info@at-service.it
A.3.1	Public cloud PII processor's purpose	AT Service utilizza i dati personali di cui è Responsabile del trattamento per le esclusive finalità necessarie all'erogazione del servizio	Nomina Responsabile trattamento
A.3.2	Public cloud PII processor's commercial use	AT Service utilizza i dati personali di cui è Responsabile del trattamento per le esclusive finalità necessarie all'erogazione del servizio	Nomina Responsabile trattamento
A.5.1	Secure erasure of temporary files	I file temporanei presenti nei sistemi di AT Service sono cancellati tempestivamente come definito nelle policy interne.	
A.6.1	PII disclosure notification	Nel caso di richieste da parte delle autorità di informazioni personali contenute del Cloud, se non configura reato, AT Service comunicherà al Cliente l'avvenuta comunicazione e la relativa autorità e motivazione.	
A.6.2	Recording of PII disclosures	AT Service si è strutturata in modo da registrare tempestivamente eventuali Data Breach e provvedere alla corretta gestione.	AT Service, al 31.12.2024 non ha registrato Data Breach.

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



A.8.1	Disclosure of sub-contracted PII processing	AT Service può utilizzare sub responsabili del trattamento per svolgere le proprie attività. AT Service conserva un registro, con relative nomine, di tutti i sub responsabili che possono essere richiesti dal Cliente in qualsiasi momento.	Nomina Responsabile Trattamento
A.10.1	Notification of a data breach involving PII	In caso di Data Breach AT Service informa tempestivamente il Cliente di quanto avvenuto e di tutti i dettagli della violazione nonché delle contromisure adottate per contenere i danni.	
A.10.2	Notification of a data breach involving PII	AT Service conserva tutta la documentazione interna (comprensiva di politiche, procedure, istruzioni, manuali, ecc.) in conformità alla normativa vigente.	
A.10.3	PII return, transfer and disposal	Alla conclusione del contratto di un Prodotto SaaS, AT Service provvede alla cancellazione e rimozione definitiva dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo PEC. AT Service gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.	
A.11.1	Confidentiality or non-disclosure agreements	Non Disclosure Agreement (NDA): AT Service sottoscrive con tutti i propri addetti (dipendenti o collaboratori) un accordo di riservatezza al fine di tutelare anche i dati personali trattati nell'ambito della collaborazione.	
A.11.2	Restriction of the creation of hardcopy material	AT Service ha definito una politica per ridurre l'utilizzo di materiale cartaceo.	
A.11.3	Control and logging of data restoration	AT Service mantiene un registro dei ripristini dati.	
A.11.4	Protecting data on storage media leaving the premises	AT Service ha definito una politica di sicurezza per il trasporto e/o trasferimento di dispositivi fisici contenenti informazioni personali che prevede tra le altre misure di sicurezza la cifratura dei dati.	
A.11.5	Use of unencrypted portable storage media and devices	AT Service ha definito una politica di sicurezza per il trasporto e/o trasferimento di dispositivi fisici contenenti informazioni personali che prevede tra le altre misure di sicurezza la cifratura dei dati.	
A.11.6	Encryption of PII transmitted over public data-transmission networks	Canale sicuro SSL - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).	
A.11.7	Secure disposal of hardcopy materials	AT Service ha definito una policy interna per la distruzione della documentazione cartacea tramite appositi distruggi documenti.	
A.11.8	Unique use of user IDs	AT Service ha definito una politica di accesso alle informazioni che prevede un ID utente distinto per ogni addetto.	
A.11.9	Records of authorized users	AT Service mantiene un registro degli accessi dettagliati per risorsa e tipologia di informazioni.	
A.11.10	User ID management	AT Service ha definito apposita policy interna per non assegnare utenti disattivi o scaduti ad altri individui.	

SICUREZZA DELLE INFORMAZIONI norma ISO 27001:2024

Aspetti di sicurezza del Cloud di AT Service Srl

CONTROLLI AGGIUNTIVI CLOUD ISO 27017 | 27018



A.11.11	Contract measures	AT Service sottoscrive la Nomina a Responsabile del Trattamento dei Dati Personali fornita dal Cliente. In assenza di questa è in grado di proporre il proprio template sottoscritto e ha inserito nell'EULA del prodotto la DPA con indicate le misure di sicurezza applicate.	Nomina Responsabile del Trattamento
A.11.12	Sub-contracted PII processing	AT Service predispone apposite nomine per Sub Responsabili del Trattamento dei Dati Personali e mantiene un registro aggiornato.	
A.11.13	Access to data on pre-used data storage space	Nel Cloud di AT Service sono previste procedure per la cancellazione delle informazioni non più utilizzate prima che sia allocato nuovamente lo spazio.	
A.12.1	Geographical location of PII	Il Cloud di AT Service e di eventuali Partner è situato in Italia o in altro paese dell'Unione Europea.	Italia
A.12.2	Intended destination of PII	Le reti del perimetro di AT Service sono sottoposte periodicamente a test di sicurezza, tra cui Vulnerability Assessment.	