Athena srl Consulenza e Servizi
Via Marinella 42/44
87046 Montalto Uffugo (CS)

POLITICA DI SICUREZZA DELLE INFORMAZIONI PER L'UTILIZZO DEL CLOUD

Doc: PSIC – Rev. 0 del 28/07/2025

Classificazione	Documento ad uso esterno
Data del documento	28/07/2025
Emesso da	RSGI

PREMESSA

L'affidamento dei dati in cloud ai sensi della Linea Guida ISO/IEC 27017 comporta la verifica di alcuni requisiti sia per il Cliente che per Athena.

Athena, in totale trasparenza per la gestione dei servizi offerti, fornisce nel seguito una sintesi degli adempimenti riferiti al Cliente e di quelli adottati da Athena in qualità di fornitore in ottemperanza alle norme UNI CEI EN ISO/IEC 27001:2024, ISO/IEC 27017 e ISO/IEC 27018.

Qualora il Cliente riscontri delle discrepanze rispetto a quanto di seguito riportato e agli eventuali servizi offerti, è invitato a segnalarle inviando una mail a serviziotecnicoathena@athenacs.it

PROTOCOLLO DEI SERVIZI CLOUD

I dati conservati nell'ambiente di cloud computing possono essere soggetti ad accesso e gestione da parte di Athena; a tutela del Cliente, Athena adotta metodi e processi certificati da enti terzi a fronte della norma UNI EN ISO/IEC 27001:2024 con estensione alle linee guida ISO/IEC 27017:2015, ISO IEC 27018:2019.

1. Athena ha individuato per la Protezione dei Dati Personali, l'Agenzia Nazionale per la Cybersicurezza e la Polizia Postale quali autorità competenti per la protezione dei dati personali.

Qualora il Cliente decida di modificare e/o integrare tali organi, è tenuto a definire preventivamente tali aspetti, in apposito accordo tra le parti.

2. Athena eroga i propri servizi cloud su infrastrutture ubicate nell'Unione Europea e gestite da Amazon Web Services (https://aws.amazon.com).

Amazon Web Services (AWS) supporta 143 standard di sicurezza e certificazioni di conformità, tra cui PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 e NIST 800-171, aiutando i clienti a soddisfare i requisiti di conformità in tutto il mondo. AWS dispone di certificazioni di conformità ISO/IEC 27001:2022, 27017:2015 e 27018:2019.

3. Athena comunicherà al Cliente con un preavviso di 30 giorni eventuali variazioni dei fornitori di cloud utilizzati. Athena garantisce che le infrastrutture che erogano i servizi cloud saranno sempre ubicate nell'Unione Europea, salvo diversa ed esplicita richiesta del Cliente, e che il trattamento dei dati sarà conforme alla Direttiva Europea sulla Protezione dei Dati (GDPR – Regolamento UE 2016/679).

4. Athena classifica tutte le informazioni scambiate con il Cliente. L'etichettatura segue i seguenti livelli di classificazione:

Categoria di informazioni	Descrizione	Esempi
Documenti ad uso esterno	Le informazioni fornite non sono riservate e pertanto possono essere pubbliche senza che ciò abbia implicazioni negative se vengono rilevate. La mancanza di disponibilità di queste informazioni in caso di tempi di inattività è un rischio accettabile. L'integrità è importante ma non fondamentale e vitale per la vita o l'attività del Cliente.	Brochure, siti web, newsletter
Documenti ad uso interno	Documentazione per uso interno che necessita di particolare protezione in quanto contiene informazioni sensibili a cui dovrebbe accedere solo un piccolo gruppo di persone autorizzate, in quanto la sua divulgazione non autorizzata potrebbe causare danni significativi all'organizzazione.	Contratti con i clienti, offerte, progetti di sviluppo servizi, progetti di sviluppo software, documenti legali interni,
Documenti Riservati	Documentazione che contiene informazioni estremamente sensibili che, se divulgate, potrebbero causare gravi danni all'organizzazione, ai suoi Clienti o ai suoi partner. L'accesso a queste informazioni è limitato a un numero molto ridotto di persone, con rigorose misure di protezione. Di questo tipo di documentazione fanno parte anche i documenti di proprietà del cliente della cui conservazione Athena è responsabile (Es. Database utenti ecc.)	Codici sorgente software, know-how utilizzato per elaborare le informazioni del Cliente, dati degli utenti del servizio, dati sanitari sensibili, chiavi crittografiche o certificati di sicurezza, informazioni finanziarie riservate

5. Il Registro dei Beni (REBE) di Athena include le informazioni e le risorse associate, comprese quelle archiviate nell'infrastruttura cloud di Athena. Il Registro dei Beni (REBE) indica dove sono conservate le risorse.

Athena srl Consulenza e Servizi
Via Marinella 42/44
87046 Montalto Uffugo (CS)

6. Athena adotta un'adeguata allocazione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni e conferma di essere in grado di adempiere ai propri ruoli e responsabilità in materia di sicurezza dei dati.

A tal fine, vengono condotte rivalutazioni periodiche dell'analisi dei rischi, delle valutazioni delle vulnerabilità e dei test di penetrazione. A tal proposito, Athena attua una propria politica per la prevenzione e la gestione delle minacce, sulla quale, su richiesta del Cliente, può fornire documentazione al riguardo.

Il Cliente che decide di modificare e/o integrare le pratiche di controllo di Athena è tenuto a definire preventivamente tali aspetti, in apposito accordo tra le parti.

7. Tutti gli accessi ai sistemi, ai servizi e all'applicativo Amalthea di Athena erogato in modalità Cloud SaaS sono sicuri e protetti. Per garantire elevati livelli di protezione e bloccare eventuali tentativi di accesso malevoli, è attivo apposito sistema di autenticazione e controllo degli accessi (userid e password).

8. La gestione del servizio cloud offerto al Cliente considera il profilo di accesso al servizio fornito da Athena. Athena comunica al Cliente le modalità standard di accesso al momento dell'attivazione del servizio.

9. Athena adotta una politica di segregazione della rete per ottenere la segregazione degli ambienti cloud dei clienti.

Nel dettaglio, l'infrastruttura Cloud garantisce la segregazione logica dei dati dei clienti dei servizi cloud, delle applicazioni virtualizzate, dei sistemi operativi, dello storage e delle reti per garantire l'integrità e la riservatezza dei dati.

10. Il Cliente deve assicurarsi che la capacità di erogazione del servizio concordata con Athena venga soddisfatta.

Athena fornisce al Cliente gli strumenti necessari per monitorare l'utilizzo del servizio e anticipare le esigenze di capacità, garantendo prestazioni ottimali dei servizi cloud richiesti nel tempo.

11. I servizi erogati sulla infrastruttura Cloud implementano controlli di crittografia, in occasione della trasmissione dati, conformi a standard di sicurezza riconosciuti e approvati.

A tal proposito Athena implementa pratiche per il controllo e il mantenimento dell'efficacia delle chiavi crittografiche durante tutto il loro ciclo di vita, compresa la generazione, l'installazione, l'aggiornamento, la revoca e la distruzione. Come prassi standard, Athena applica controlli crittografici a tutte le transazioni da e verso il Cliente tramite protocollo https e/o sftp.

12. Athena mantiene politiche e procedure scritte specifiche per lo smaltimento o il riutilizzo sicuro delle risorse. Su esplicita richiesta del Cliente, Athena è disponibile a fornire tali documenti.

13. Le credenziali di accesso ai servizi applicativi forniti dalla infrastruttura Cloud sono univoche per ogni utente e non possono essere condivise.

Athena srl Consulenza e Servizi
Via Marinella 42/44
87046 Montalto Uffugo (CS)

Classificazione	Documento ad uso esterno
Data del documento	28/07/2025
Emesso da	RSGI

Le credenziali non devono essere conservate su supporti scritti in modo da facilitare l'accesso non autorizzato da parte di terzi.

14. Per i servizi applicativi forniti dalla Infrastruttura Cloud, Athena offre un servizio di backup come previsto dal contratto con il Cliente.

Salvo diverso accordo con il Cliente, la politica di backup prevede che tutti i backup (log applicativi, db e repository documentale) siano effettuati con cadenza giornaliera.

Salvo diverse necessità da parte del Cliente e opportunamente comunicate, è garantita la conservazione dei backup relativi agli ultimi 6 mesi di utilizzo

I backup vengono archiviati in almeno 3 data center in modo ridondante, fornendo una resilienza integrata contro i disastri diffusi.

15. Athena testa i backup dei database e verifica lo stato di allineamento delle replicazioni documentali giornalmente secondo quanto riportato nella procedura "Dump & Restore" per garantirne l'integrità e l'affidabilità per ripristini sicuri e senza compromessi.

I log sono archiviati su una piattaforma centralizzata che garantisce che siano immutabili e non possano essere eliminati, nemmeno accidentalmente.

16. Tutte le attività relative alla risoluzione dei problemi di sicurezza e al miglioramento dell'usabilità dei servizi forniti dalla Infrastruttura Cloud sono condotte dal personale Athena con le autorizzazioni e le deleghe appropriate. L'accesso viene registrato con il timestamp.

17. Per i servizi erogati dalla Infrastruttura Cloud, i clock di sistema sono sincronizzati con fonti approvate.

Questa sincronizzazione viene eseguita regolarmente per garantire timestamp accurati per le attività di elaborazione, registrazione e controllo dei dati.

18. Il Cliente deve determinare i requisiti di sicurezza delle informazioni e quindi valutare se i servizi offerti da Athena soddisfano tali requisiti. A tal fine, il Cliente ha la facoltà di richiedere ad Athena informazioni sulle funzionalità di sicurezza delle informazioni adottate.

19. Athena conduce le operazioni di sviluppo in un ambiente sicuro e dedicato utilizzando dati di test non di produzione. Tali operazioni sono disciplinate da specifiche procedure scritte. Athena può fornire documentazione su tale processo su esplicita richiesta del Cliente.

20. Il Cliente deve includere Athena nella propria politica di sicurezza delle informazioni, nei rapporti con i fornitori. Ciò contribuirà a mitigare i rischi associati all'accesso e alla gestione dei dati gestiti nei servizi offerti da Athena.

Athena srl Consulenza e Servizi
Via Marinella 42/44
87046 Montalto Uffugo (CS)

Classificazione	Documento ad uso esterno
Data del documento	28/07/2025
Emesso da	RSGI

21. Il Cliente deve confermare i ruoli e le responsabilità in merito alla sicurezza delle informazioni relative ai servizi forniti da Athena e descritti nel relativo contratto.
22. Athena dispone di una procedura scritta specifica per la gestione degli incidenti di sicurezza delle informazioni.

Questa politica garantisce un approccio coerente ed efficace alla risoluzione di tali incidenti, comprese le comunicazioni relative agli eventi di sicurezza.

La politica mira a mitigare i seguenti rischi:

- Ridurre l'impatto delle violazioni della sicurezza delle informazioni assicurando che gli incidenti siano seguiti correttamente.
- Aiutare a identificare le aree di miglioramento per ridurre il rischio e l'impatto di incidenti futuri, diminuendo la superficie di attacco e le possibilità di violazioni dei dati.

Gli incidenti di sicurezza delle informazioni devono essere segnalati il prima possibile inviando una e-mail a serviziotecnicoathena@athenacs.it. A seguito della verifica dell'incidente, il personale responsabile valuterà la situazione e metterà in atto opportune azioni correttive e/o misure di contenimento.

In caso di data breach, questo dovrà essere segnalato al DPO di Athena (dpo@athenacs.it), che attiverà la specifica procedura operativa di Athena per la gestione dei data breach. Ciò include la tempestiva comunicazione della violazione all'Autorità Garante per la Protezione dei Dati Personali e ai responsabili della commessa (Cliente).

Verrà creato un "Rapporto di incidente" per gli incidenti di sicurezza delle informazioni.

Un "Incidente di Sicurezza delle Informazioni" è un evento che ha causato o ha il potenziale di causare danni agli asset, alla reputazione e/o ai Clienti di Athena. Tali incidenti includono, a titolo esemplificativo ma non esaustivo:

- la perdita o il furto di dati o informazioni;
- il trasferimento di dati o informazioni a coloro che non hanno il diritto di ricevere tali informazioni;
- tentativi (falliti o riusciti) di ottenere l'accesso non autorizzato ai file di dati o informazioni di un sistema informatico di Athena o dei suoi Clienti;
- modifiche fraudolente di informazioni o dati in un sistema informatico;
- interruzione non richiesta di un servizio fornito dalla Infrastruttura Cloud;
- l'azione di malware o di un attacco DDOS.

Il Cliente deve fornire le seguenti informazioni essenziali:

- se la perdita di dati mette a rischio qualsiasi persona o altri dati;

Athena srl Consulenza e Servizi
Via Marinella 42/44
87046 Montalto Uffugo (CS)

- la data e l'ora in cui si è verificato l'incidente di sicurezza.

È quindi fondamentale che il Cliente identifichi qualsiasi punto debole relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei servizi forniti da Athena.

Athena risponderà agli incidenti di sicurezza delle informazioni in conformità con le procedure documentate.

Le conoscenze acquisite dall'analisi e dalla risoluzione degli incidenti di sicurezza delle informazioni saranno utilizzate da Athena per ridurre la probabilità o l'impatto di incidenti futuri.

23. La trasmissione dei dati gestiti sulla Infrastruttura Cloud è crittografata utilizzando protocolli di crittografia sicuri come TLS.

24. In caso di forza maggiore, calamità naturali, atti terroristici o qualsiasi altro evento catastrofico ragionevolmente imprevedibile che abbia un impatto sull'infrastruttura sottostante la Infrastruttura Cloud, Athena si riserva il diritto di migrare i servizi forniti al Cliente ad un altro fornitore certificato ISO 27001, ISO 27017 e ISO 27018, a condizione che il servizio di Disaster Recovery sia incluso nel contratto con il Cliente.

25. I dati trattati dal Cliente in qualità di Titolare del trattamento sull'Infrastruttura Athena Cloud rimarranno sempre di proprietà del Cliente.

26. Athena, in ottemperanza al Regolamento UE 2016/679 (GDPR), garantisce al titolare del trattamento la possibilità di ricevere in qualsiasi momento una copia dei dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico ("diritto di accesso"), nonché di conoscere il luogo fisico in cui risiedono i dati.

27. Athena garantisce la portabilità dei dati che saranno restituiti al titolare in uno dei formati più comuni (es. CSV) secondo quanto riportato nella procedura di reversibilità del servizio erogato in modalità Clous SaaS disponibile su richiesta del cliente.

28. Athena, in ottemperanza al Regolamento UE 2016/679 (GDPR), garantisce al titolare del trattamento la cancellazione dei propri dati ("diritto all'oblio") secondo quanto riportato nella procedura di reversibilità del servizio erogato in modalità Clous SaaS.

Il diritto alla cancellazione prevale sull'interesse alla conservazione dei dati. In tali casi, se un titolare del trattamento richiede la cancellazione dei propri dati, Athena procederà senza ingiustificato ritardo e non si riserverà il diritto di continuare a trattare i dati fino alla scadenza originariamente stabilita, indipendentemente dal fatto che tale scadenza sia imminente o meno.

29. Athena, in qualità di responsabile del trattamento di dati personali in cloud, si impegna a includere nei suoi contratti con i clienti una disposizione che richiede la notifica di qualsiasi richiesta legalmente vincolante per la divulgazione di informazioni di dati personali da parte delle autorità preposte all'applicazione della legge. Athena fornirà tali notifiche in conformità con le procedure e i tempi concordati stabiliti nel contratto, a meno

che non sia vietato dall'autorità preposta all'applicazione della legge di divulgare tali informazioni. Ciò garantisce che i clienti siano informati e possano intraprendere le azioni appropriate in merito a qualsiasi richiesta di divulgazione di dati personali.

30. Athena ha una procedura specifica in merito alla restituzione, al trasferimento e/o all'eliminazione di dati personali. In caso di esplicita richiesta da parte del Cliente, Athena è disponibile a fornire tale documento.

31. È responsabilità del Cliente richiedere una descrizione documentata del processo di cessazione del servizio cloud fornito da Athena, che comprende la rimozione degli eventuali asset del Cliente seguita dall'eliminazione di tutte le copie di tali asset dai sistemi di Athena. A tal fine, Athena dispone di una procedura scritta specifica per la disattivazione di un servizio, comprese le modalità di restituzione dei dati.

32. Athena si impegna a garantire che tutte le informazioni, i concetti, le idee, le procedure, i metodi e i dati tecnici di cui il proprio personale venga a conoscenza durante l'erogazione dei servizi al Cliente siano trattati in modo confidenziale e soggetto a segretezza.

Athena adotta con i propri collaboratori tutte le cautele necessarie per tutelare la riservatezza di tali informazioni e documentazione. Inoltre, Athena aderisce alla normativa in materia di trattamento dei dati personali e rispetta i diritti delle persone fisiche e di altri soggetti in conformità al Codice in materia di protezione dei dati personali (D.Lgs. 196/03 e successive modifiche) e al Regolamento 2016/679 e sue applicazioni.

Qualora il Cliente ritenga opportuno richiedere prove documentate dell'attuazione di specifici controlli di sicurezza relativi ai servizi forniti da Athena, e qualora ciò non rappresenti un rischio per la sicurezza delle informazioni di Athena e/o dei suoi Clienti, tali documenti saranno classificati come "Riservati" e forniti al Cliente.

33. Athena garantisce che, una volta deallocato, l'ambiente cloud del Cliente venga completamente eliminato e tutti i dati vengano completamente cancellati prima che le risorse vengano ridistribuite o riassegnate. Questo processo garantisce che non rimangano dati residui.

34. Tutte le comunicazioni effettuate da Athena avvengono tramite protocollo HTTPS, SSL e TLS, garantendo che i dati trasmessi raggiungano la destinazione corretta.

35. Athena garantisce l'uso limitato di materiali stampati, i quali vengono distrutti mediante triturazione quando non sono più necessari.

36. Athena garantisce che le copie delle politiche di sicurezza e delle procedure operative siano conservate per un periodo di almeno 5 anni.

37. Il Cliente deve considerare che le leggi e i regolamenti applicabili possono includere quelli che regolano sia la giurisdizione di Athena che le sue attività.