SISTEMA DI GESTIONE DEL SERVIZIO

DATA VISION S.R.L.

DOPOS

Documento Politica

per la Gestione del Servizio

Sistema di Gestione del Servizio conforme alla norma ISO/IEC 20000-1

La presente revisione allinea la politica al quadro delle sedici politiche di sicurezza informatica adottate da Data Vision in attuazione della misura GV.PO-01 della Determinazione ACN n. 164179/2025, con particolare riguardo al requisito DE.CM-01 punto 2, che assegna ai livelli di servizio attesi anche la funzione di strumento per il rilevamento tempestivo degli incidenti significativi.

Codice DOC: 02DIMS
Livello di riservatezza 0 - Pubblico Informazioni di pubblico accesso.
Dati pubblicati su internet o destinati alla pubblica diffusione.

Revisione	Data di revisione	Redatta da	Verificata da	Approvata
Revisione 1.2 – Settembre 2026. La revisione integra il Sistema di Gestione del Servizio con il quadro di conformità NIS2 di Data Vision, esplicita il ruolo dei livelli di servizio ai fini del rilevamento tempestivo degli incidenti significativi, raccorda i processi di gestione degli incidenti, delle modifiche, della capacità e dei fornitori alle politiche di sicurezza informatica adottate per i sedici ambiti della misura GV.PO-01, e corregge i riferimenti al Sistema di Gestione per la Continuità Operativa erroneamente presenti nella precedente revisione in luogo di quelli al Sistema di Gestione del Servizio. Correzioni redazionali. I valori puntuali dei livelli di servizio, gli indicatori di prestazione e i parametri operativi sono riservati e sono trattati nel Piano di Gestione del Servizio, nel Manuale Operativo del Servizio e negli accordi contrattuali, classificati Livello 1 – Uso interno.	Ottobre 2026	RRSG Elena Amendola	RSG Daniel Bizzarro	RDSG Valerio Bizzarro

Lista di distribuzione: Pubblicazione su sito web aziendale
A:
Al personale Data Vision Ai fornitori, ai partner dei servizi in outsourcing, ai Clienti e a tutti coloro che sono coinvolti o svolgono un ruolo definito nei Sistemi di Gestione adottati da Data Vision.

Cronologia delle revisioni				
Revisione	**Data di revisione**	**Redatta da**	**Verificata da**	**Approvata**
Rilascio 1.1 Aggiornamento ISO 27001	Gennaio 2024	RRSG Elena Amendola	RSG Daniel Bizzarro	RDSG Valerio Bizzarro
Rilascio 1.0 Prima stesura	Febbraio 2023	RRSG Elena Amendola	RSG Daniel Bizzarro	RDSG Valerio Bizzarro

Sommario

1. Scopo, campo di applicazione e destinatari 4
2. Impegno della Direzione 4
3. La politica per la gestione del servizio 6
3.1. Obiettivi 6
3.2. Misure di controllo 7
4. Il Sistema di Gestione del Servizio e la conformità NIS2 8
4.1. Data Vision quale soggetto NIS 8
4.2. Livelli di servizio attesi e rilevamento degli incidenti significativi 8
4.3. Gestione degli incidenti di servizio e incidenti di sicurezza 9
4.4. Gestione delle modifiche 9
4.5. Capacità, disponibilità e continuità del servizio 9
4.6. Fornitori e catena di approvvigionamento 9
4.7. Servizi erogati a Clienti soggetti NIS 9
4.8. Quadro di raccordo con le politiche di sicurezza informatica 11
5. Comunicazione della politica 13
6. Ruoli, responsabilità e autorità 13
7. Piano di Gestione del Servizio (SM Plan) 15
8. Documenti correlati 15
9. Riferimenti normativi 16
10. Riesame 16

1. SCOPO, CAMPO DI APPLICAZIONE E DESTINATARI

Data Vision ha definito ed implementato un Sistema di Gestione del Servizio IT (SMS), basato sui requisiti definiti dalla norma ISO/IEC 20000-1 (Information technology – Service management), sul perimetro costituito dalle attività di progettazione e sviluppo di soluzioni applicative software e relativa assistenza e di erogazione di consulenza e servizi a supporto dei Clienti.

La presente Politica è applicata a tutte le sedi, le strutture, le attività, i prodotti e i servizi nel campo di applicazione dei Sistemi di Gestione citati.

La responsabilità della gestione di questo documento è del Responsabile dei Sistemi di Gestione ed è approvata dal Comitato Guida.

I destinatari di questo documento sono tutti i dipendenti di Data Vision, così come tutti i fornitori, i partner dei servizi in outsourcing, i Clienti e tutti quelli che sono coinvolti e/o svolgono un ruolo definito nei Sistemi di Gestione adottati da Data Vision.

Il Sistema di Gestione del Servizio opera all'interno del Sistema di Gestione Integrato di Data Vision, che comprende altresì il Sistema di Gestione per la Qualità conforme alla norma UNI EN ISO 9001, il Sistema di Gestione per la Sicurezza delle Informazioni conforme alla norma UNI CEI ISO/IEC 27001, il Sistema di Gestione per la Continuità Operativa conforme alla norma ISO 22301 e il Sistema di Gestione Ambientale conforme alla norma UNI EN ISO 14001.

2. IMPEGNO DELLA DIREZIONE

L'Alta Direzione si impegna a soddisfare i requisiti di tutte le parti interessate e a migliorare continuamente il Sistema di Gestione del Servizio. L'impegno della Direzione si attua:

- assicurando che siano stabiliti la politica e gli obiettivi per la Gestione del Servizio e che essi siano adeguati e compatibili con gli indirizzi strategici e lo scopo dell'organizzazione, e fornendo servizi di manutenzione e supporto dell'infrastruttura in base agli SLA secondo i requisiti del Cliente, nel rispetto della legislazione e dei regolamenti nazionali applicabili;
- assicurando l'integrazione dei requisiti del SMS nei processi di business dell'organizzazione;
- assicurando la disponibilità delle risorse necessarie al SMS, tramite la messa a disposizione dei mezzi tecnici, economici e delle risorse umane necessarie;
- assicurando che il SMS consegua i risultati attesi;
- guidando e supportando il personale affinché contribuisca con impegno quotidiano all'efficacia del SMS;
- promuovendo il miglioramento continuo;
- fornendo supporto agli altri ruoli manageriali rilevanti per dimostrare la loro leadership e il loro impegno nelle rispettive aree di responsabilità;

- assicurando che il Sistema di Gestione del Servizio concorra al soddisfacimento degli obblighi gravanti su Data Vision quale soggetto NIS, secondo quanto previsto al capitolo 4;
- verificando la Politica periodicamente nel corso del riesame del SMS.

3. LA POLITICA PER LA GESTIONE DEL SERVIZIO

Il Sistema di Gestione del Servizio IT è implementato e mantenuto secondo i requisiti specificati dall'insieme delle procedure operative e sottoposto a revisione su base periodica regolare per garantirne la conformità agli obblighi di legge, ai regolamenti e alle norme volontarie applicate. Attraverso tale insieme di procedure:

- sono identificati i processi, i servizi e i fattori coinvolti nell'erogazione, valutati per criticità e documentati sulla base di requisiti normativi, contrattuali, delle esigenze di business e delle regole interne;
- è stabilita, documentata e testata periodicamente la pianificazione del servizio IT, assicurando l'efficacia e l'aggiornamento continuo delle soluzioni tecniche e organizzative adottate.

Il personale è adeguatamente formato sulla politica di Gestione del Servizio IT affinché contribuisca consapevolmente e responsabilmente alla sua applicazione e al miglioramento continuo del SMS. A tale scopo è garantita l'adeguatezza e l'aggiornamento periodico e regolare dei piani di formazione per il personale e per le altre eventuali entità coinvolte, quali le parti terze e i subappaltatori con un ruolo critico nell'erogazione dei servizi, che devono essere informati e conformi alla presente politica aziendale. I contenuti formativi in materia di sicurezza informatica sono erogati secondo la politica POL-FC e il relativo piano di formazione.

3.1. Obiettivi

La pianificazione degli obiettivi determina le attività che devono essere effettuate, le responsabilità di attuazione, i tempi di completamento, le risorse necessarie e le modalità di verifica dei risultati. Data Vision ha fissato obiettivi generali e specifici, misurabili, definiti e documentati nelle procedure del SMS, e si propone principalmente il soddisfacimento delle esigenze di servizio dei propri Clienti, in termini di implementazioni e supporto e in conformità con i requisiti dello specifico SLA. Con l'attuazione della Politica del SMS, Data Vision si impegna a:

- garantire il rispetto dei livelli di servizio concordati con i Clienti per i servizi che rientrano nell'ambito, nonché a gestire possibili incidenti, richieste e problemi;
- definire un sistema per rilevare, analizzare, segnalare e correggere eventuali carenze o violazioni degli accordi sul livello di servizio concordati con i propri Clienti;
- migliorare la comunicazione tra il personale che partecipa alla fornitura dei servizi ed i Clienti e utenti di detti servizi;
- aumentare l'efficienza dei processi di fornitura e supporto per il miglioramento dei servizi esistenti;
- assicurare che i livelli di servizio attesi siano definiti e documentati anche ai fini del rilevamento tempestivo degli incidenti significativi, secondo quanto previsto al paragrafo 4.2.

Per garantire il raggiungimento degli obiettivi, Data Vision ha definito politiche e procedure per monitorare continuamente l'efficacia del Sistema di Gestione dei Servizi, rivedendo se necessario gli obiettivi di qualità e di gestione del servizio.

3.2. Misure di controllo

In particolare, la Direzione ha adottato le seguenti principali misure di controllo.

Misure di controllo del rischio. Finalizzate alla mitigazione e al contenimento sia della probabilità di accadimento di eventuali incidenti, sia della capacità di impatto. La Metodologia di Valutazione e Trattamento del Rischio adottata da Data Vision (S010) identifica gli elementi di rischio che possono mettere a repentaglio il ripristino dell'operatività e definisce i livelli di rischio accettabili sia ai fini della norma ISO 22301 sia, in ambito sicurezza delle informazioni, della norma UNI CEI ISO/IEC 27001 , ed è altresì il riferimento metodologico della politica POL-RC per la gestione del rischio di cybersecurity.

Piano per la Continuità delle Attività aziendali. Considera i rischi identificati e le strategie per contrastarli, minimizzando l'interruzione del lavoro e assicurando un rapido ripristino delle attività. Il Piano di Disaster Recovery consente a Data Vision di affrontare eventi avversi, garantendo il ripristino dei servizi critici in tempi e con modalità che limitano le conseguenze dell'impatto negativo. Entrambi sono disciplinati dalla politica POL-BC / DOPOR e dalla procedura S006.

Procedura di Gestione degli Incidenti. Adeguata a riconoscere, comunicare e rispondere agli incidenti in modo efficace ed appropriato contenendone l'impatto. La procedura S004 disciplina unitariamente gli incidenti di servizio e gli incidenti di sicurezza informatica, ivi compresi gli obblighi di notifica al CSIRT Italia, in attuazione della politica POL-RI.

Le responsabilità e i metodi per misurare se gli obiettivi sono stati raggiunti sono specificati nel Piano di Gestione del Servizio (SM Plan).

4. IL SISTEMA DI GESTIONE DEL SERVIZIO E LA CONFORMITÀ NIS2

4.1. Data Vision quale soggetto NIS

Dal 12 aprile 2025, con Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, Data Vision S.r.l. è stata inserita nell'elenco dei soggetti NIS ai sensi dell'articolo 7, comma 3, lettera a) del Decreto legislativo 4 settembre 2024, n. 138, ed individuata quale soggetto Importante. In attuazione della misura GV.PO-01 della Determinazione ACN n. 164179/2025, Data Vision ha adottato sedici politiche di sicurezza informatica, una per ciascuno degli ambiti ivi individuati.

Il presente capitolo, introdotto con la revisione 1.2, non modifica l'impianto del Sistema di Gestione del Servizio conforme alla norma ISO/IEC 20000-1, che resta invariato. Esso esplicita in quali punti i processi del SMS concorrono al soddisfacimento degli obblighi NIS2 e come essi si raccordano alle politiche di sicurezza informatica adottate. I requisiti NIS2 si aggiungono ai requisiti delle certificazioni già conseguite e non li sostituiscono.

4.2. Livelli di servizio attesi e rilevamento degli incidenti significativi

Il punto 2 della misura DE.CM-01 dell'Allegato 1 alla Determinazione ACN n. 164179/2025, obbligatorio per i soggetti importanti, richiede che siano definiti e documentati i livelli di servizio attesi dei servizi e delle attività del soggetto NIS "anche ai fini di rilevare tempestivamente gli incidenti significativi". Il livello di servizio assume pertanto, accanto alla funzione di impegno contrattuale verso il Cliente, quella di strumento di rilevamento.

Uno scostamento significativo rispetto al livello atteso — un degrado delle prestazioni, un aumento anomalo dei tempi di risposta, un incremento improvviso del volume di segnalazioni, l'indisponibilità di una componente — può costituire il primo indicatore disponibile di un incidente in corso, anche prima che sia generato un allarme dagli strumenti di sicurezza. Il Sistema di Gestione del Servizio è, sotto questo profilo, esso stesso un presidio di sicurezza.

Conseguentemente, e in raccordo con la politica POL-MO relativa all'ambito o) "Monitoraggio degli eventi di sicurezza":

- per ciascun servizio e attività rilevante sono definiti e documentati i parametri che ne esprimono il livello di erogazione atteso e le soglie il cui superamento determina la generazione di una segnalazione;
- il perimetro comprende sia i livelli di servizio concordati contrattualmente con i Clienti sia i livelli di servizio interni, poiché la norma si riferisce ai servizi e alle attività del soggetto NIS e non ai soli servizi oggetto di contratto;
- lo scostamento dal livello atteso è valutato anche in chiave di sicurezza e, ove ne ricorrano i presupposti, è instradato senza ritardo verso il processo di gestione degli incidenti di cui alla procedura S004;
- i livelli di servizio e le relative soglie sono riesaminati almeno annualmente in sede di riesame del SMS, anche alla luce degli esiti del monitoraggio e degli incidenti occorsi.

Il Piano di Gestione del Servizio, il Manuale Operativo del Servizio e gli accordi contrattuali costituiscono, unitamente al presente documento, l'evidenza documentale di conformità al requisito DE.CM-01 punto 2.

4.3. Gestione degli incidenti di servizio e incidenti di sicurezza

Il processo di gestione degli incidenti del SMS e il processo di gestione degli incidenti di sicurezza informatica sono unificati nella procedura S004, così da evitare che un evento pervenuto al Service Desk quale disservizio non sia riconosciuto quale possibile incidente di sicurezza. Ogni segnalazione è qualificata secondo i criteri della procedura S004 e della Tassonomia Cyber dell'Agenzia per la Cybersicurezza Nazionale; la qualificazione dell'incidente come significativo ai sensi dell'Allegato 3 alla Determinazione ACN e i conseguenti obblighi di notifica al CSIRT Italia sono disciplinati dalla politica POL-RI e dalla procedura S004.

La comunicazione ai destinatari dei servizi degli incidenti significativi che possono ripercuotersi negativamente sulla fornitura, nonché delle minacce significative e delle relative misure correttive o di mitigazione, è disciplinata dalla politica POL-RI in attuazione della misura RS.CO-02 e costituisce parte integrante degli obblighi informativi verso i Clienti del SMS.

4.4. Gestione delle modifiche

Il processo di gestione delle modifiche del SMS costituisce il presidio attraverso il quale sono autorizzate, tracciate e verificate le transizioni di stato dei sistemi informativi e di rete disciplinate dalla politica POL-SM: introduzione, riconfigurazione, aggiornamento, sostituzione, trasferimento e dismissione. Le modifiche alle basi di regole dei sistemi perimetrali e ai flussi di rete autorizzati sono del pari trattate quali modifiche, secondo la politica POL-RE e la procedura S011. Ove la modifica incida su sistemi informativi e di rete rilevanti, è preceduta dalla valutazione del rischio secondo la procedura S010.

4.5. Capacità, disponibilità e continuità del servizio

I processi di gestione della capacità e della disponibilità del servizio concorrono alla resilienza operativa richiesta dall'articolo 24, comma 2, lettera c) del Decreto legislativo n. 138/2024 e si raccordano alla politica POL-BC e alla procedura S006 per la continuità operativa e il ripristino in caso di disastro, nonché alla procedura S007 per il salvataggio e il ripristino dei dati e delle configurazioni. Le esigenze di continuità individuate nei piani costituiscono il riferimento per la definizione dei livelli di servizio attesi in condizioni degradate.

4.6. Fornitori e catena di approvvigionamento

Il processo di gestione dei fornitori e delle parti esterne del SMS si raccorda alla politica POL-CA in materia di rischi per la sicurezza informatica della catena di approvvigionamento ICT. I fornitori e i partner dei servizi in outsourcing con un ruolo critico nell'erogazione sono censiti negli inventari di cui alla politica POL-AM, sono soggetti agli obblighi contrattuali di sicurezza previsti dalla politica POL-CA e sono tenuti a comunicare tempestivamente gli incidenti che possano ripercuotersi sui servizi erogati a Data Vision e, per il tramite di questa, ai Clienti.

4.7. Servizi erogati a Clienti soggetti NIS

Data Vision opera quale fornitore di servizi gestiti (MSP) e di servizi gestiti di sicurezza (MSSP). Ove il Cliente sia a sua volta soggetto NIS, i servizi erogati da Data Vision concorrono al soddisfacimento degli obblighi gravanti sul

Cliente. Ove il Cliente sia qualificato quale soggetto essenziale, Data Vision assicura contrattualmente anche il soddisfacimento dei requisiti dell'Allegato 2 alla Determinazione ACN pertinenti al servizio erogato, che in tal caso assumono natura vincolante nei limiti dell'oggetto del contratto. Le misure che Data Vision adotta in via volontaria quale soggetto importante sono espressamente qualificate come tali nelle rispettive politiche.

La rendicontazione ai Clienti dei servizi erogati e dei livelli di servizio conseguiti, ivi compresa quella riferita ai servizi dichiarati all'Agenzia per la Cybersicurezza Nazionale, è parte del processo di reportistica del servizio ed è svolta con la periodicità stabilita contrattualmente.

4.8. Quadro di raccordo con le politiche di sicurezza informatica

La tabella seguente riporta, per ciascuno dei sedici ambiti della misura GV.PO-01, la politica adottata da Data Vision e il punto di contatto con il Sistema di Gestione del Servizio. Il raccordo non trasferisce al SMS obblighi che restano in capo alle rispettive politiche, ma individua i processi del servizio attraverso i quali tali obblighi trovano attuazione operativa.

Amb.	Politica	Codice	Punto di contatto con il SMS
a)	Gestione del rischio	02DI-RC_POL-001	Valutazione del rischio a supporto delle decisioni di progettazione, transizione e modifica dei servizi (S010).
b)	Ruoli e responsabilità	02DI-RR_POL-002	Assegnazione delle responsabilità e delle autorità del SMS, coerente con la matrice RACI della sicurezza informatica.
c)	Affidabilità delle risorse umane	02DI-RU_POL-003	Requisiti di affidabilità del personale che opera sui servizi e sui sistemi dei Clienti.
d)	Conformità e audit di sicurezza	02DI-CO_POL-004	Audit Interno (PGO3) e Riesame della Direzione (PGO1), estesi al SMS.
e)	Catena di approvvigionamento ICT	02DI-CA_POL-005	Processo di gestione dei fornitori e delle parti esterne (par. 4.6).
f)	Gestione degli asset	02DI-AM_POL-006	Inventari degli asset, dei servizi e dei servizi erogati dai fornitori a supporto della configurazione del servizio (S008).
g)	Gestione delle vulnerabilità	02DI-VU_POL-007	Pianificazione degli interventi di aggiornamento quali modifiche, nel rispetto dei livelli di servizio (S009).
h)	Continuità operativa, DR e crisi	02DI-BC_POL-008-BC	Disponibilità e continuità del servizio; livelli di servizio in condizioni degradate (par. 4.5, S006).
i)	Autenticazione e controllo accessi	02DI-AC_POL-009	Gestione delle utenze e degli accessi degli operatori del servizio e degli amministratori nominati per Cliente (S002).
j)	Sicurezza fisica	02DI-SF_POL-010	Protezione dei locali e del data center dai quali il servizio è erogato (S001, S005).
k)	Formazione e consapevolezza	02DI-FC_POL-011	Formazione del personale del servizio e delle parti terze con ruolo critico (cap. 3, PGO2, PIANO-FC).
l)	Sicurezza dei dati	02DI-SI_POL-012	Protezione dei dati dei Clienti trattati nell'erogazione del servizio.
m)	Sviluppo, configurazione, manutenzione e dismissione dei sistemi	02DI-SM_POL-013	Processo di gestione delle modifiche e di rilascio; configurazione dei sistemi di servizio (par. 4.4, PFO5, S007).
n)	Protezione delle reti e delle comunicazioni	02DI-RE_POL-014	Modifiche alle regole perimetrali e ai flussi autorizzati; canali di comunicazione con i Clienti (S011).
o)	Monitoraggio degli eventi di sicurezza	02DI-MO_POL-015	Livelli di servizio attesi quale strumento di rilevamento; reportistica di servizio (par. 4.2).

Amb.	Politica	Codice	Punto di contatto con il SMS
p)	Risposta agli incidenti e ripristino	02DI-RI_POL-016	Processo unificato di gestione degli incidenti di servizio e di sicurezza (par. 4.3, S004).

5. COMUNICAZIONE DELLA POLITICA

La politica per la gestione del servizio è:

- resa disponibile come informazione documentata;
- comunicata all'interno dell'organizzazione;
- resa disponibile alle parti interessate, per quanto appropriato.

La comunicazione della presente Politica è effettuata all'interno dell'azienda e, ove necessario, alle parti interessate. Il Responsabile dei Sistemi di Gestione è responsabile della comunicazione. Allo scopo, la presente Politica è comunicata a tutti i dipendenti e collaboratori e pubblicata integralmente sul sito aziendale a disposizione delle parti interessate.

La Direzione e il Responsabile del SMS devono assicurare che la Politica per la Gestione del Servizio sia compresa ed attuata da tutto il personale nello svolgimento della propria attività. In caso di cambiamenti a qualsiasi livello, sono valutati gli impatti sulla sicurezza delle informazioni, garantendone la completa ed efficace gestione.

6. RUOLI, RESPONSABILITÀ E AUTORITÀ

La Direzione assicura che le responsabilità e le autorità per i ruoli pertinenti siano assegnate e comunicate all'interno dell'organizzazione. A tale scopo la Direzione ha definito e formalizzato la struttura organizzativa, i ruoli e le responsabilità nell'ambito della gestione del servizio, promuovendo il coinvolgimento di tutte le funzioni aziendali. La Direzione ha assegnato le responsabilità e le autorità per:

- assicurare che il SMS sia conforme ai requisiti del presente documento;
- riferire alla Direzione sulle prestazioni del SMS.

Data Vision, prima di eseguire le modifiche necessarie al SMS, ne garantisce lo scopo e considera le conseguenze potenziali dei cambiamenti proposti. Il Responsabile del SMS si occupa di verificare l'efficienza dei servizi forniti e delle rispettive risorse attraverso rapporti di servizio, sondaggi sulla soddisfazione del Cliente e analisi dei reclami e dei riscontri positivi dei Clienti; di pianificare eventuali cambiamenti necessari al SMS; di monitorare eventuali non conformità, falsi allarmi, incidenti e altri eventi rilevanti. Si impegna inoltre a misurare i risultati e il raggiungimento degli obiettivi almeno una volta all'anno durante l'Audit Interno e ha la responsabilità del Riesame periodico. Gli obiettivi e i corrispondenti risultati sono rivisti dalla Direzione di Data Vision almeno una volta all'anno durante il Riesame della Direzione, attraverso metodi di misurazione documentati.

Ai fini della conformità NIS2, il Responsabile del SMS definisce e documenta i livelli di servizio attesi di cui al paragrafo 4.2 e ne assicura la disponibilità ai fini del monitoraggio, in raccordo con il Responsabile del SGSI e con il CSM / Responsabile Gestione Rischi. Il Punto di Contatto NIS2 mantiene i rapporti con l'Agenzia per la Cybersicurezza Nazionale e con il CSIRT Italia. Non esiste in Data Vision una figura di CISO: la responsabilità ultima

della sicurezza informatica è in capo all'Amministratore Delegato, che si avvale delle funzioni individuate dalla politica POL-RR.

I ruoli del SMS e le relative responsabilità e autorità sono descritti nel Piano di Gestione del Servizio.

Il Responsabile del SMS si occupa del presente documento, verificandolo periodicamente e, se necessario, aggiornandolo almeno una volta all'anno.

7. PIANO DI GESTIONE DEL SERVIZIO (SM PLAN)

Data Vision ha definito e documentato un piano di gestione del servizio che viene rivisto annualmente. In esso sono pianificati tutti i compiti necessari nell'anno in corso per la progettazione, l'implementazione, il funzionamento, la manutenzione e il supporto del sistema di gestione dei servizi.

Il piano di gestione del servizio definisce gli obiettivi annuali di gestione del servizio, che devono essere allineati con gli obiettivi generali descritti nella presente politica, e riporta i livelli di servizio attesi con i relativi parametri e soglie di cui al paragrafo 4.2.

Come allegati al piano di gestione del servizio sono incluse anche le evidenze dell'attuazione del piano, del monitoraggio e della revisione (analisi degli indicatori, audit di sistema e revisioni del sistema) e del miglioramento continuo.

L'attuazione della presente Politica per la Gestione del Servizio IT è sottoposta in modo trasparente alla verifica dei Clienti, ed eventuali altre parti interessate, ed è controllata in modo oggettivo da un Ente di Certificazione indipendente.

La Direzione, condividendo i principi e gli obiettivi per una corretta politica finalizzata alla Gestione del Servizio IT che garantisca la sicurezza delle informazioni e la resilienza operativa, approva ed emette il presente documento di Politica per la Gestione del Servizio e supporta pienamente il programma per la sua attuazione e il suo mantenimento, richiamando su questi aspetti l'attenzione del proprio personale, dei collaboratori, dei fornitori e dei Clienti.

8. DOCUMENTI CORRELATI

- Piano di Gestione del Servizio (SM Plan) e Manuale Operativo del Servizio (01MO);
- Manuale Integrato dei Sistemi di Gestione (MISiGe, 01MA);
- 02DI-MO_POL-015– Politica per il Monitoraggio degli Eventi di Sicurezza (02DI-MO);
- 02DI-RI_POL-016– Politica per la Risposta agli Incidenti e il Ripristino, e S004 con playbook, istruzioni operative e registro;
- 02DI-BC_POL-008-BC– Politica per la Continuità Operativa, il Ripristino in caso di Disastro e la Gestione delle Crisi, e S006;
- 02DI-SM_POL-013– Politica per lo Sviluppo, la Configurazione, la Manutenzione e la Dismissione dei Sistemi Informativi e di Rete, e procedure PFO5 e S007;
- 02DI-RE_POL-014– Politica per la Protezione delle Reti e delle Comunicazioni, e S011;

- 02DI-AC_POL-009, 02DI-AM_POL-006, 02DI-VU_POL-007, 02DI-SI_POL-012, 02DI-SF_POL-010, 02DI-CA_POL-005, 02DI-RC_POL-001, 02DI-RR_POL-002, 02DI-RU_POL-003, 02DI-FC_POL-011, 02DI-CO_POL-004 e le relative procedure;
- 02DI-Q_PoliticaQualità; DOPOA – Politica Integrata Ambientale e Carbon Footprint;
- 04DI – DOSI; 06DI – Regolamento Disciplinare Tecnico; PGO1 – Riesame della Direzione; PGO3 – Audit Interno.

9. RIFERIMENTI NORMATIVI

- ISO/IEC 20000-1 – Sistemi di gestione del servizio;
- UNI EN ISO 9001; UNI CEI ISO/IEC 27001 ; ISO 22301; UNI EN ISO 14001;
- Direttiva (UE) 2022/2555 (NIS2);
- Decreto legislativo 4 settembre 2024, n. 138, in particolare articoli 24 e 25;
- Determinazione ACN n. 164179/2025, Allegati 1, 2 e 3, con particolare riguardo alle misure GV.PO-01, DE.CM-01 e RS.CO-02;
- Linee Guida NIS dell'Agenzia per la Cybersicurezza Nazionale e Tassonomia Cyber ACN.

10. RIESAME

La presente Politica è riesaminata e, se opportuno, aggiornata periodicamente e comunque almeno con cadenza annuale in sede di Riesame della Direzione, nonché qualora si verifichino modifiche significative dei servizi erogati, variazioni organizzative, evoluzioni del contesto normativo o incidenti significativi. Il riesame verifica almeno la permanenza dell'adeguatezza dei livelli di servizio attesi e delle relative soglie, la coerenza con le politiche di sicurezza informatica adottate in attuazione della misura GV.PO-01 e l'efficacia del raccordo di cui al paragrafo 4.8.