REGIONE BASILICATA

DIREZIONE GENERALE
AMMINISTRAZIONE DIGITALE

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

REGIONE BASILICATA

Direzione Generale Amministrazione Digitale

Condizioni di utilizzo dei servizi del Data Center Unico Regionale

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

SOMMARIO

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

1. CONTESTO DI RIFERIMENTO

La Regione Basilicata, ai sensi del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale – CAD) e in attuazione della Strategia Cloud Italia nonché del Regolamento ACN in materia di infrastrutture digitali e servizi cloud per la Pubblica Amministrazione, ha realizzato il Data Center Unico Regionale, destinato all'erogazione di servizi cloud in favore degli Enti e delle Società pubbliche del territorio regionale.

Il Data Center costituisce il nodo strategico del sistema informativo pubblico regionale, volto a favorire il processo di innovazione organizzativa e digitale e a promuovere un uso efficace ed efficiente delle infrastrutture tecnologiche nel rispetto dei principi di razionalizzazione, interoperabilità, sicurezza, continuità operativa e sovranità del dato.

L'infrastruttura, realizzata in conformità allo standard ANSI-TIA 942 - Livello 3, è gestita nel rispetto dei requisiti di sicurezza, resilienza, continuità operativa e protezione dei dati personali stabiliti dalla normativa nazionale ed europea vigente.

2. DEFINIZIONI E ACRONIMI

2.1. DEFINIZIONI

Termine	Descrizione
Regione Basilicata (o Regione)	L'Amministrazione regionale, incluse le strutture operative preposte all'erogazione e alla gestione dei Servizi (Direzione Amministrazione Digitale o l'Ufficio preposto nella stessa incardinato, COC, SOC, CSIRT)
Utente	L'Ente o la Società pubblica del territorio regionale che sottoscrive la Convenzione e fruisce dei Servizi
Fornitore	Soggetto privato contrattualizzato dall'Utente per l'utilizzo e/o la gestione dei Servizi. Il Fornitore non è parte del presente accordo; il suo operato ricade sotto l'esclusiva responsabilità dell'Utente
Parti	La Regione Basilicata e l'Utente
Servizi	I servizi IT erogati dalla Regione Basilicata, come descritti nel *"Catalogo dei servizi del Data Center Unico Regionale"*
Servizi IaaS (Infrastructure as a Service)	Modello di servizio cloud che prevede l'allocazione di sole risorse elaborative di base (CPU, RAM e Storage)
SLA (Service Level Agreement)	Indicatori oggettivi e misurabili di disponibilità e prestazione del Servizio
Amministratore di sistema	Figura professionale che gestisce e sovrintende ai Servizi

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

2.2. ACRONIMI

Termine	Descrizione
COC	Cloud Operations Center
SOC	Security Operations Center
CSIRT	Computer Security Incident Response Team
ACN	Agenzia per la Cybersicurezza Nazionale

3. RIFERIMENTI

3.1. RIFERIMENTI NORMATIVI

- **D.Lgs. 196/2003 e ss.mm.ii, noto come Codice in materia di protezione dei dati personali:** principale legge italiana che regola il trattamento dei dati personali;
- **Regolamento UE 2016/679** o **GDPR (General Data Protection Regulation**): misure tecniche e organizzative adeguate a garantire la sicurezza dei dati che le aziende devono implementare;
- **Direttiva NIS2:** ufficialmente conosciuta come **Direttiva (UE) 2022/2555**, revisione e ampliamento della **Direttiva NIS** (Network and Information Security) del 2016. La direttiva mira a rafforzare ulteriormente la resilienza e la sicurezza informatica all'interno dell'UE, affrontando le crescenti minacce cyber nei settori critici;
- **Regolamento unico per le infrastrutture digitali e i servizi cloud della Pubblica Amministrazione**, adottato dall'Agenzia per la Cybersicurezza Nazionale (ACN) il 27 giugno 2024 (prot. n. 0021007.27-06-2024.I);
- **D. Lgs. 4 settembre 2024, n. 138:** recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. (24G00155);
- **D. Lgs. 82/2005 e ss.mm.ii.,** "Codice dell'Amministrazione digitale";
- **D. Lgs. 81/2008 e ss.mm.ii**., "Testo Unico sulla sicurezza";
- **Provvedimento del Garante 27 novembre 2008**: misure di sicurezza che devono essere adottate per la gestione dei Log degli amministratori di sistema;
- **Provvedimento del Garante n. 209/2021** sulla procedura telematica per la notifica dei data breach;

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

- **Deliberazione D.G.R. n. 43 del 01/02/2023**, con la quale la Regione Basilicata ha aderito al modello di qualificazione della ACN (Agenzia per la Cybersicurezza Nazionale) n. 307 del 18 gennaio 2022 e n. 29 del 2 gennaio 2023 e con decreto direttoriale n. 21007/24 del 27 giugno 2024 (regolamento unico per le infrastrutture e i servizi cloud per la PA);
- **Deliberazione D.G.R. n. 483 del 10/08/2023**, con la quale la Regione Basilicata ha ammesso a finanziamento il potenziamento dei servizi di Disaster Recovery, a seguito delle nuove linee guida ACN;
- **D.D. n.16BJ.2024/D.01076 del 27/12/2024** con la quale la Regione Basilicata ha istituito un centro di competenze per la risposta agli incidenti informatici con il compito di pianificare ed eseguire attività di sicurezza proattive e reattive volte a prevenire e rispondere attacchi informatici all'interno del territorio regionale;
- **Deliberazione D.G.R. n. 724 del 27/11/2025**, "Governance delle infrastrutture e dei servizi digitali della Regione Basilicata".
- **Deliberazione D.G.R. n. 46 del 10/03/2026**, "Approvazione del Sistema di Gestione della Sicurezza Informatica (SGSI) della Regione Basilicata".

3.2. STANDARD DI SETTORE

- **NIST SP800-92 - Guide to Computer Security Log Management:** pubblicazione riconosciuta a livello internazionale che fornisce raccomandazioni e linee guida per la gestione dei log di sicurezza informatica;
- **ISO/IEC 27001:2022**: standard internazionale pubblicato dall'**International Organization for Standardization (ISO)** e dall'**International Electrotechnical Commission (IEC)** che definisce i requisiti per un **Sistema di Gestione della Sicurezza delle Informazioni** (**ISMS**, Information Security Management System). La versione 2022 aggiorna la precedente ISO/IEC 27001:2013. Questo standard richiede che le organizzazioni adottino controlli per la protezione delle informazioni, tra cui l'uso di meccanismi crittografici per garantire la riservatezza, l'integrità e la disponibilità dei dati;
- **ISO/IEC 27002:2022**: standard internazionale complementare a ISO/IEC 27001 che fornisce linee guida dettagliate per l'implementazione delle misure di sicurezza dell'informazione. Offre una serie di raccomandazioni e best practice per applicare i controlli di sicurezza previsti da ISO/IEC 27001, inclusi quelli relativi alla gestione dei Log (Log management);
- **COBIT "Control Objectives for Information and related Technology" (modello di riferimento per il governo dell'IT)**: framework progettato per la governance e la gestione dell'IT, che include la gestione della sicurezza delle informazioni.

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

3.3. SEZIONE INFORMATIVA DI RIFERIMENTO

- **Catalogo dei servizi del Data Center Unico Regionale:** https://www.regione.basilicata.it/?temi-dgad=infrastrutture-digitali/data-center
- **Standard tecnologici:** https://www.regione.basilicata.it/?temi-dgad=infrastrutture-digitali/data-center
- **Manuale di gestione della sicurezza informatica:** https://www.regione.basilicata.it/?temi-dgad=cybersicurezza

4. OGGETTO E AMBITO DI APPLICAZIONE

Le presenti condizioni di utilizzo costituiscono parte integrante e sostanziale della convenzione per la condivisione di risorse tecnologiche e servizi del Data Center Unico Regionale e disciplinano in modo vincolante i rapporti tra la Regione Basilicata e l'Utente secondo il modello di responsabilità condivisa ("shared responsibility model") tipico dei servizi cloud, nel quale la ripartizione delle responsabilità varia in funzione del modello di servizio attivato, come meglio specificato nel *"Catalogo dei Servizi del Data Center Unico Regionale"*.

L'attivazione dei Servizi implica, da parte dell'Utente, l'accettazione integrale delle presenti condizioni, degli *"Standard tecnologici"*, delle misure riportate nel *"Manuale di gestione della sicurezza informatica"* e delle direttive della Regione. L'Utente dovrà rispondere di eventuali danni, malfunzionamenti o inadempimenti causati dal mancato rispetto delle suddette prescrizioni, il tutto come di seguito dettagliato.

Per quanto non espressamente riportato all'interno delle presenti condizioni di utilizzo, si fa espresso rinvio alle norme di legge vigenti.

5. MODALITÀ OPERATIVE E COMUNICAZIONE TRA LE PARTI

A seguito della sottoscrizione della presente Convenzione, le richieste di attivazione, modifica o dismissione dei Servizi devono essere presentate dal Legale rappresentante/Amministratore, dal Dirigente competente, dal RUP o da un funzionario/dipendente indicato dall'Utente come referente unico per il servizio tramite la piattaforma dedicata o, in via residuale, tramite PEC all'indirizzo della Direzione Generale Amministrazione Digitale.

Non è in alcun caso ammesso l'invio di richieste incomplete o la richiesta di soluzioni, anche temporanee, che non rispettino gli *"Standard tecnologici"*, le misure riportate nel

"Manuale di gestione della sicurezza informatica" (Allegato A.3) e le direttive della Regione, nonché la normativa vigente.

L'Utente è responsabile del corretto dimensionamento dei Servizi richiesti in base alle proprie necessità, fermo restando il supporto della Regione in fase di valutazione e definizione dei fabbisogni.

La Regione, tramite la Direzione Amministrazione Digitale o l'Ufficio preposto nella stessa incardinato, eseguirà l'istruttoria amministrativa e tecnica dell'istanza nel rispetto dei principi di imparzialità e buon andamento e potrà chiedere integrazioni o rigettare la richiesta fornendo all'Utente opportuna motivazione. Tale iter si applica anche ad eventuali richieste di modifica o integrazione di Servizi già in uso, che saranno valutate caso per caso.

Ai fini dell'istruttoria, la Regione potrà richiedere all'Utente informazioni relative agli eventuali Fornitori terzi incaricati della gestione e/o della manutenzione dei Servizi concessi in uso, ivi incluse le principali informazioni relative al contratto in essere, con particolare riferimento alla durata e alle modalità di erogazione del servizio. Con riferimento, in particolare, ai Servizi di Hosting e IaaS, sarà richiesta la documentazione tecnica relativa agli applicativi che si intende installare sull'infrastruttura regionale, nonché i relativi codici sorgente, al fine di consentire le necessarie verifiche tecniche e di sicurezza sugli applicativi stessi. Nel caso di software distribuito in licenza d'uso o comunque non nella disponibilità dell'Utente, quest'ultimo dovrà fornire ogni elemento utile allo svolgimento delle verifiche di sicurezza, ivi incluse, ove disponibili, le Software Bill of Materials (SBOM) o altra documentazione tecnica equivalente resa disponibile dal produttore o dal Fornitore del software. Resta ferma la facoltà della Regione di richiedere ulteriori informazioni o evidenze tecniche ritenute necessarie ai fini della valutazione. Potrà altresì essere richiesto il coinvolgimento del Fornitore dell'Utente per eventuali approfondimenti tecnici e verifiche di sicurezza sugli applicativi.

6. OBBLIGHI E FACOLTÀ DELLE PARTI

L'Utente prende atto e accetta:

- che la Regione Basilicata fornisce i Servizi indicati nel *"Catalogo dei servizi del Data Center Unico Regionale"* e nel rispetto degli *"Standard tecnologici"* definiti. È responsabilità esclusiva dell'Utente valutare l'adeguatezza dei Servizi rispetto ai propri scopi o esigenze;
- che la Direzione Generale Amministrazione Digitale o l'Ufficio preposto nella stessa incardinato eseguirà l'istruttoria amministrativa e tecnica dell'istanza e potrà chiedere integrazioni o rigettare la richiesta fornendo opportuna motivazione;

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

- che eventuali richieste di modifica o integrazione di Servizi già in uso saranno valutate secondo lo stesso iter previsto per le nuove richieste;
- che eventuali richieste non compatibili con i requisiti tecnici e/o con le disponibilità dell'infrastruttura regionale (ad es. in termini di risorse elaborative o di licenze d'uso) potranno essere rigettate ovvero, qualora tecnicamente realizzabili, essere accolte subordinatamente alla preventiva definizione delle modalità di copertura degli eventuali costi aggiuntivi a carico dell'Utente, da disciplinare mediante specifico atto integrativo o attuativo della convenzione;
- che la Regione si riserva il diritto di sospendere o interrompere l'erogazione dei Servizi, ovvero di inibirne l'accesso da Internet, in caso di violazione da parte dell'Utente dei termini, delle condizioni e/o degli obblighi previsti dalla convenzione, dal presente documento e/o da quelli ivi richiamati, secondo quanto previsto dal successivo art. 20;
- di essere responsabile:
    - dei contenuti e dei dati inseriti e/o resi disponibili all'interno dei Servizi concessi in uso e comunque, a qualsiasi titolo, trasmessi, diffusi o messi online dall'Utente stesso o dal Fornitore dallo stesso incaricato;
    - dei malfunzionamenti dei Servizi per qualsiasi uso non conforme alle presenti condizioni di utilizzo, agli *"Standard tecnologici"* e alle misure riportate nel *"Manuale di gestione della sicurezza informatica"*, nonché alla normativa vigente;
    - nel caso dei Servizi IaaS, di eventuali malfunzionamenti dei software installati dall'Utente o su sua richiesta, nonché dei danni dagli stessi eventualmente derivanti.

L'Utente si obbliga, altresì:

- a richiedere esclusivamente Servizi che siano funzionali alle attività istituzionali, nel rispetto delle leggi vigenti e della proprietà intellettuale;
- a utilizzare esclusivamente i canali individuati dalla Regione per l'attivazione, la modifica e la dismissione di Servizi e a presentare istanze complete in tutte le loro parti;
- a designare un referente unico che costituisca il punto di contatto per le comunicazioni tra l'Utente e la Regione;

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

- a garantire le dotazioni strumentali, tecnologiche ed organizzative, nonché le competenze tecniche necessarie per il corretto utilizzo, l'amministrazione e la gestione dei Servizi concessi in uso, nel rispetto degli standard di qualità e sicurezza;
- a garantire la continuità del contratto di assistenza con l'eventuale Fornitore incaricato della gestione o dell'utilizzo dei Servizi per suo conto;
- a garantire la piena conformità agli *"Standard tecnologici"* e alle misure riportate nel *"Manuale di gestione della sicurezza informatica"*, nonché l'adeguamento ad eventuali modifiche delle stesse che dovessero occorrere nel tempo;
- ove del caso, a comunicare l'eventuale presenza di trattamenti di dati personali appartenenti a categorie particolari, ai sensi dell'articolo 9 del Regolamento (UE) 2016/679 (GDPR);
- a informare tempestivamente la Regione di eventuali irregolarità o malfunzionamenti dei Servizi, impegnandosi a fornire tutte le informazioni necessarie alla loro risoluzione. Le segnalazioni saranno prese in carico dalla Regione compatibilmente con le risorse disponibili e secondo le priorità tecniche e organizzative del servizio. I tempi di presa in carico e di gestione delle richieste possono variare in funzione, tra l'altro, della tipologia di intervento, dell'ordine di arrivo e del grado di priorità della segnalazione;
- a richiedere tempestivamente la disattivazione dei Servizi che non siano più necessari;
- ad osservare la massima riservatezza rispetto alle informazioni e ai dati di cui dovesse venire a conoscenza durante la fruizione dei Servizi;

La Regione:

- si riserva la facoltà di verificare che i Servizi richiesti corrispondano alle effettive esigenze dell'Utente;
- garantisce la fornitura dei Servizi previsti nel *"Catalogo dei servizi del Data Center Unico Regionale"*, in conformità agli *"Standard tecnologici"* e alle misure riportate nel *"Manuale di gestione della sicurezza informatica"*;
- assicura la manutenzione dell'infrastruttura fisica e virtuale e implementa le misure tecniche e organizzative necessarie a garantirne il corretto funzionamento e la sicurezza attraverso le proprie strutture operative (Direzione Amministrazione Digitale o l'Ufficio preposto nella stessa incardinato, COC, SOC, CSIRT);

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

- non sosterrà alcun onere per Servizi e licenze che non siano esplicitamente previsti nel *"Catalogo dei servizi del Data Center Unico Regionale"* e negli *"Standard tecnologici"*;
- non è soggetta ad alcun obbligo generale di sorveglianza sui comportamenti e gli atti posti in essere dall'Utente e/o dal suo Fornitore, né controlla informazioni, dati e contenuti immessi all'interno dei Servizi concessi in uso; tuttavia, si riserva di cancellare contenuti di cui venga a conoscenza e che ritenga offensivi o che violino leggi o diritti di terzi. Rispetto a questo tipo di contenuti, la Regione Basilicata si riserva inoltre il diritto di agire a tutela dei propri interessi;
- si riserva la facoltà di modificare in qualsiasi momento le presenti condizioni di utilizzo, il *"Catalogo dei servizi del Data Center Unico Regionale"*, gli *"Standard tecnologici"* e il *"Manuale di gestione della sicurezza informatica"*. Le modifiche possono comportare, tra l'altro, l'introduzione, l'aggiornamento, la sostituzione o la dismissione di specifiche tipologie di Servizi. Qualora tali modifiche comportino la necessità di adeguamenti tecnici o derivino da sopravvenute disposizioni normative con impatto sui Servizi concessi in uso, la Regione ne darà comunicazione all'Utente. Gli eventuali adeguamenti richiesti dovranno essere effettuati entro il termine massimo di 30 giorni dalla comunicazione, salvo diverso termine concordato tra le Parti;
- in caso di dismissione di una tipologia di Servizio, darà preventiva comunicazione all'Utente, indicando, ove possibile, eventuali soluzioni alternative o le modalità e i tempi di cessazione del Servizio.

Per quanto non espressamente riportato nelle presenti condizioni e nei documenti in esse richiamati, si rinvia alle norme di legge vigenti.

7. ACCESSO AI SERVIZI

L'accesso remoto ai Servizi per attività di manutenzione e assistenza tecnica o, ove del caso, per la semplice fruizione degli stessi, è consentito esclusivamente tramite connessioni VPN (Virtual Private Network) configurate secondo standard di sicurezza adeguati, che prevedono autenticazione multi-fattore (MFA), cifratura dei dati in transito e meccanismi di controllo dell'integrità del traffico di rete. La Regione si riserva di adottare ulteriori misure di sicurezza, quali limitazioni per indirizzo IP, segmentazione di rete, controllo degli endpoint e sistemi di monitoraggio degli accessi privilegiati, in coerenza con la normativa vigente in materia di cybersicurezza e protezione dei dati.

Le credenziali di accesso nominative rilasciate hanno carattere strettamente personale, non sono cedibili né divulgabili e devono essere utilizzate esclusivamente dal soggetto

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

autorizzato. Gli accessi e le operazioni effettuate mediante tali credenziali sono attribuite al relativo titolare e sono oggetto di registrazione e monitoraggio mediante sistemi di logging conformi alla normativa vigente.

I permessi di accesso vengono disabilitati in caso di scadenza della Convenzione, cessazione o variazione del rapporto di lavoro del soggetto autorizzato (ivi compreso il personale di eventuali Fornitori dell'Utente), nonché in caso di uso improprio, smarrimento, divulgazione o accertata violazione delle presenti condizioni, delle misure riportate nel *"Manuale di gestione della sicurezza informatica"* o della normativa vigente in materia di cybersicurezza e protezione dei dati. Eventuali utilizzi non autorizzati o illeciti sono perseguibili ai sensi della normativa applicabile.

La protezione delle credenziali e degli eventuali codici di autenticazione deve essere assicurata dall'Utente mediante l'adozione di adeguate misure organizzative e tecniche, secondo le migliori pratiche di sicurezza informatica; ogni evento di smarrimento, compromissione o utilizzo non autorizzato deve essere tempestivamente comunicato alla Regione, così come eventuali variazioni relative al personale autorizzato all'accesso.

La Regione può sospendere o limitare gli accessi qualora ciò sia necessario per garantire la sicurezza dell'infrastruttura regionale, nel rispetto dei principi di proporzionalità e leale collaborazione istituzionale.

8. AMMINISTRAZIONE DEI SERVIZI

La Regione mantiene il pieno controllo tecnico e amministrativo dei Servizi concessi in uso all'Utente, riservandosi la facoltà di operare in autonomia per lo svolgimento, a titolo esemplificativo, di attività di gestione, manutenzione, aggiornamento, hardening, monitoraggio e messa in sicurezza dell'infrastruttura e delle componenti di base, anche ai fini del rispetto degli obblighi in materia di cybersicurezza, continuità operativa e protezione dei dati. La Regione informerà preventivamente l'Utente laddove l'intervento possa comportare impatti sull'operatività dei Servizi, salvo i casi di urgenza indifferibile connessi alla sicurezza dei sistemi, alla gestione di vulnerabilità critiche o alla tutela del perimetro infrastrutturale regionale.

La suddivisione delle responsabilità per tipologia di Servizio è riportata nel *"Catalogo dei servizi del Data Center Unico Regionale"*.

In particolare, nel caso di servizi IaaS, l'Utente, anche laddove gli vengano assegnati permessi amministrativi, si obbliga a non modificare o rimuovere le configurazioni di base dell'infrastruttura assegnata, ivi inclusi i sistemi di sicurezza, gli agent di monitoraggio, gli strumenti di logging o altri componenti di protezione installati dalla Regione, senza preventiva autorizzazione scritta della stessa. Eventuali software installati autonomamente

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

dall'Utente o su sua richiesta dovranno essere legittimamente licenziati, ove previsto, costantemente aggiornati e configurati in conformità alle policy di sicurezza regionali e agli standard tecnologici adottati dalla Regione. I relativi costi restano a carico dell'Utente, che si assume ogni responsabilità in ordine alla loro conformità normativa e alla compatibilità con l'infrastruttura regionale. L'Utente si obbliga inoltre a non installare software o versioni diverse da quelle concordate, sottoposte a preventiva analisi da parte della Regione e da questa formalmente approvate. È fatto divieto all'Utente di installare o mantenere in esercizio, sui Servizi concessi in uso, sistemi operativi o software per i quali il produttore abbia dichiarato la cessazione del supporto tecnico e degli aggiornamenti di sicurezza (End of Life – EOL o End of Support – EOS), nonché aventi funzionalità sovrapponibili o interferenti con i software o i sistemi gestiti dalla Regione Basilicata, con particolare riferimento alle attività di monitoraggio e cybersicurezza, salvo preventiva autorizzazione della Regione. Qualora venga rilevata la presenza di tali componenti, la Regione ne darà comunicazione all'Utente richiedendo l'adozione delle necessarie misure di aggiornamento, sostituzione o migrazione entro un termine congruo stabilito dalla Regione stessa. Decorso inutilmente tale termine, la Regione potrà adottare le misure tecniche ritenute necessarie alla mitigazione del rischio, ivi inclusa la limitazione della connettività, l'isolamento delle risorse interessate o la sospensione del Servizio, secondo quanto previsto al successivo art. 20.

Tutte le modifiche critiche ai sistemi devono essere effettuate di concerto con la Regione, a seguito di formale richiesta da parte dell'Utente. Tali interventi prevedono l'esecuzione di un backup pre-modifica e la possibilità di effettuare il rollback entro 24 ore. Gli interventi eseguiti senza il preventivo coinvolgimento della Regione escludono qualsiasi responsabilità della stessa per eventuali malfunzionamenti, danni o perdite di dati.

9. MONITORAGGIO DELLE SOGLIE DI UTILIZZO

La Regione Basilicata monitora in modalità H24/365 lo stato di utilizzo delle risorse assegnate. In caso di rilevamento di saturazione delle stesse, provvede, ove possibile e nel più breve tempo, all'incremento per la quota minima necessaria ad evitare l'interruzione del Servizio e allerta l'Utente. L'assegnazione di tali risorse aggiuntive dovrà essere limitata al tempo strettamente necessario all'Utente per effettuare, con il supporto della Regione, l'analisi della causa dell'evento, nonché per definire il piano di rientro nelle soglie previste in fase di richiesta del Servizio o per richiedere formalmente una modifica del dimensionamento delle risorse stesse che sarà valutata dalla Regione.

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

10. ANALISI DELLE VULNERABILITÀ

La Regione Basilicata effettua un monitoraggio continuo della propria infrastruttura al fine di individuare e prevenire potenziali rischi in materia di cybersicurezza, con riferimento ai livelli applicativo, infrastrutturale e di rete. In tale ambito, la Regione svolge con cadenza periodica attività di Vulnerability Assessment (VA) e Penetration Test (PT), finalizzate alla rilevazione di eventuali vulnerabilità di sicurezza.

Tali attività possono comprendere, a titolo esemplificativo e non esaustivo, scansioni automatiche di vulnerabilità, analisi delle configurazioni, verifiche di esposizione dei servizi in rete, test di intrusione, controlli finalizzati all'individuazione di anomalie o comportamenti potenzialmente dannosi per l'infrastruttura o per altri Utenti.

Le attività possono essere effettuate esclusivamente dalla Regione o da soggetti da essa incaricati, che provvederanno a comunicare preventivamente all'Utente le modalità, i tempi e il perimetro di intervento. Gli esiti delle verifiche saranno altresì condivisi con l'Utente, richiedendo, ove necessario, la predisposizione di un piano di risoluzione delle criticità riscontrate, proporzionato ai rischi individuati.

L'Utente espressamente acconsente allo svolgimento delle suddette attività e prende atto e accetta che le stesse, per loro intrinseca natura, potrebbero determinare malfunzionamenti, rallentamenti, crash di sistema, riavvii forzati, perdita o corruzione di dati, indisponibilità temporanea dei Servizi, alterazioni di configurazioni, interruzioni operative, danni indiretti o consequenziali. L'Utente prende atto, altresì, che tali attività potrebbero richiedere, in particolare nel caso di Servizi IaaS, un proprio intervento ovvero l'intervento dell'eventuale Fornitore incaricato della gestione dei Servizi per conto dell'Utente, ai fini del ripristino del regolare funzionamento dei sistemi. A tal fine, l'Utente si obbliga a garantire la continuità del contratto di assistenza con il proprio Fornitore.

Prima dell'avvio delle verifiche, nel caso in cui i sistemi siano in housing presso il Data Center Unico Regionale oppure ospitati presso i Data Center dell'Utente, quest'ultimo si obbliga a:

- effettuare backup completi e aggiornati dei sistemi e dei dati oggetto di test;
- verificare la corretta eseguibilità delle procedure di ripristino.

In ogni caso, l'Utente dovrà:

- comunicare alla Regione eventuali vincoli operativi o finestre temporali critiche;
- assicurare, nel caso in cui il servizio sia gestito da Fornitori, il necessario supporto per ripristinare i sistemi in caso di malfunzionamenti o danni.

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

La Regione Basilicata esercita le proprie funzioni con la diligenza richiesta dalla natura della prestazione adottando misure tecniche e organizzative adeguate e coerenti con le Linee Guida ACN/NIS2 in materia di gestione del rischio cyber, misure di sicurezza e gestione degli incidenti. Le verifiche di sicurezza sono pianificate ed eseguite in modalità controllata, nel rispetto del principio di necessità e proporzionalità, con l'obiettivo di ridurre al minimo gli impatti sull'operatività ordinaria dei sistemi.

Tutte le attività saranno registrate tramite log di accesso, log di comando, report tecnici e tracciabilità completa delle operazioni, ai fini di accountability e sicurezza.

Al termine delle verifiche, la Regione fornisce all'Utente:

- un report tecnico dettagliato, con evidenza delle vulnerabilità e delle configurazioni critiche riscontrate;
- raccomandazioni operative e prioritarie per la mitigazione delle vulnerabilità, con indicazioni sulle eventuali azioni correttive e sui tempi di remediation.

In presenza di vulnerabilità classificate come Critiche, la Regione potrà applicare misure temporanee di mitigazione, quali, a titolo esemplificativo, la configurazione o l'aggiornamento delle ACL, incluso il filtraggio degli indirizzi IP (ad es. Geo IP Filtering). In ogni caso, la Regione si riserva il diritto di sospendere o interrompere l'erogazione dei Servizi, ovvero inibirne l'accesso da Internet, al fine di tutelare l'integrità e la sicurezza dell'infrastruttura, come previsto al successivo art. 19.

11. GESTIONE DEI LOG

La Regione detiene e gestisce i log, differenziati in base alla tipologia di Servizio erogato, per finalità di sicurezza, monitoraggio, prevenzione degli abusi e adempimento degli obblighi normativi. Essi vengono raccolti in modalità centralizzata mediante sistemi di Security Information and Event Management (SIEM), e conservati attraverso misure tecniche idonee a garantirne integrità, immodificabilità e accesso riservato al personale autorizzato.

I log possono essere messi a disposizione dell'Utente e delle competenti Autorità giudiziarie o di pubblica sicurezza a fronte di richiesta formalmente valida ai sensi della normativa vigente.

Il periodo minimo di conservazione è pari a:

- 6 mesi per i log degli amministratori di sistema;
- 12 mesi per i log di sicurezza e autenticazione;

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

- 6 mesi per i log applicativi, sulla base del rischio,

decorsi i quali i log potranno essere cancellati o anonimizzati, salvo diversi obblighi di legge o su richiesta dell'Autorità giudiziaria.

12. GESTIONE DEGLI INCIDENTI

La Regione Basilicata dispone di un processo strutturato per la gestione tempestiva degli incidenti di sicurezza attraverso le strutture regionali CSIRT, SOC e COC, garantendo un servizio di intervento in modalità H24/365.

Eventuali incidenti di sicurezza che possano compromettere la continuità dei Servizi o la sicurezza dei dati devono essere comunicati all'altra Parte entro un tempo congruo e comunque nei termini previsti dalla normativa NIS2 e GDPR. In tale ambito, le Parti devono cooperare attivamente nello scambio tempestivo e reciproco di informazioni rilevanti per la gestione dell'incidente in termini di svolgimento delle verifiche, notifica al Garante della Privacy e/o CSIRT Italia e ripristino dell'operatività dei Servizi.

Ai fini della Direttiva NIS2 e della normativa in materia di protezione dei dati personali (GDPR), la Regione opera quale Responsabile del trattamento con riferimento ai servizi infrastrutturali e di gestione del Data Center Unico Regionale, mentre l'Utente assume il ruolo di Titolare del trattamento per i dati personali trattati mediante i Servizi.

In caso di incidente significativo ai sensi del Decreto legislativo 138/2024, la Regione provvede alle notifiche di propria competenza verso CSIRT Italia per gli eventi che incidono sull'infrastruttura del Data Center Unico Regionale. L'Utente, informato dalla Regione nei tempi previsti dalla normativa vigente, resta responsabile, in qualità di Titolare del trattamento, dell'eventuale notifica di violazione dei dati personali al Garante per la protezione dei dati personali.

Il modello di gestione degli incidenti adottato dalla Regione Basilicata è riportato nel paragrafo *"6.13 - Gestione degli incidenti e delle vulnerabilità"* del *"Manuale di gestione della sicurezza informatica"*, al quale si rimanda.

13. LIVELLI DI SERVIZIO (SLA)

Gli SLA applicabili a ciascuna classe di Servizio sono definiti nel *"Catalogo dei servizi del Data Center Unico Regionale"*. Si precisa che, ai fini del calcolo della disponibilità dei Servizi, sono escluse interruzioni o disfunzioni dovute a cause di forza maggiore, a interventi urgenti per ragioni di sicurezza, a malfunzionamenti imputabili all'Utente, nonché agli interventi di manutenzione programmata.

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

14. GESTIONE DEI BACKUP

La strategia di protezione dei dati prevede il salvataggio dei backup su una SAN dedicata presso il sito primario, con replica automatica su una SAN secondaria per finalità di Disaster Recovery. La policy di conservazione è basata su un ciclo di backup settimanali completi e incrementali giornalieri, con una retention (periodo di conservazione) di 15 giorni. Periodicamente, almeno ogni sei mesi, è previsto un test di restore con registrazione del risultato sul Sistema Di Gestione della Sicurezza Informatica in uso presso il CTR (SGSI).

Le suddette procedure di backup non si applicano ai servizi in housing presso il Data center regionale, la cui gestione è interamente in capo all'Utente.

Per ulteriori dettagli si rimanda al paragrafo *"6.14 - Gestione dei backup"* del *"Manuale di gestione della sicurezza informatica"*.

15. BUSINESS CONTINUITY E DISASTER RECOVERY

I servizi ospitati presso il Data center regionale sono sottoposti a misure di Disaster Recovery e Continuità Operativa.

Nel caso di Servizi IaaS, è onere dell'Utente configurare i propri applicativi affinché siano compatibili con le architetture di alta disponibilità messe a disposizione dalla Regione.

Per ulteriori dettagli si rimanda al paragrafo *"6.15 - Business continuity e Disaster recovery"* del *"Manuale di gestione della sicurezza informatica"*.

16. FORNITORI TERZI

Qualora l'Utente conceda a soggetti terzi l'utilizzo dei Servizi messi a disposizione dalla Regione o si avvalga di un Fornitore esterno per la loro gestione, è fatto obbligo all'Utente, ove ne ricorrano i presupposti, di nominare il Fornitore quale Responsabile del trattamento dei dati, ai sensi dell'art. 28 GDPR, nonché a vigilare sul rispetto di tutte le prescrizioni contenute nelle presenti condizioni, negli *"Standard tecnologici"*, nelle misure previste dal *"Manuale di gestione della sicurezza informatica"*, nelle direttive regionali e nella normativa vigente, provvedendo altresì, ove possibile, a inserire nei propri contratti di appalto specifiche clausole vincolanti in tal senso.

In ogni caso, l'Utente resta l'unico responsabile nei confronti della Regione per i Servizi concessi in uso e risponderà di eventuali danni, malfunzionamenti o disservizi derivanti

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

da una negligente condotta del Fornitore e/o dal mancato rispetto delle suddette prescrizioni (culpa in vigilando).

Al fine di assicurare il costante presidio dei Servizi nonché lo svolgimento delle necessarie attività di gestione e, ove del caso, di manutenzione, l'Utente si obbliga a garantire la continuità del contratto di assistenza con il proprio Fornitore e a vigilare sul relativo operato.

17. AUDIT

La Regione Basilicata si riserva il diritto di effettuare, direttamente o tramite soggetti incaricati e vincolati da obblighi di riservatezza, verifiche e audit tecnici, organizzativi e documentali sugli ambienti, sulle configurazioni e sulle modalità di utilizzo dei Servizi da parte dell'Utente, al fine di accertarne la conformità alle presenti condizioni di utilizzo, agli *"Standard tecnologici"*, alle misure riportate nel *"Manuale di gestione della sicurezza informatica"*, ai termini della convenzione, nonché alla normativa vigente in materia di cybersicurezza, protezione dei dati personali e continuità operativa, ivi inclusa la disciplina di recepimento della Direttiva (UE) 2022/2555 (NIS2), i regolamenti e le disposizioni emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN), il Regolamento (UE) 2016/679 (GDPR), il Codice dell'Amministrazione Digitale e gli standard internazionali applicabili alla sicurezza delle informazioni e dei servizi cloud (tra cui ISO/IEC 27001 e correlate).

Le attività di audit sono finalizzate alla tutela dell'integrità, disponibilità e riservatezza dell'infrastruttura regionale, nonché alla prevenzione di rischi sistemici o vulnerabilità suscettibili di impattare altri Utenti. L'Utente si impegna a collaborare attivamente, fornendo accesso alla documentazione tecnica e organizzativa pertinente, ad eventuali log e a tutte le informazioni necessarie per lo svolgimento delle verifiche, nel rispetto dei principi di proporzionalità, pertinenza e minimizzazione. In caso di non conformità o situazioni di rischio per la sicurezza dell'infrastruttura, la Regione potrà richiedere l'attuazione di misure correttive entro termini congrui ovvero, nei casi di urgenza o grave criticità, adottare misure tecniche proporzionate e temporanee di limitazione o sospensione dei Servizi come specificato nel successivo art. 19, fermo restando l'obbligo di motivazione e il rispetto dei principi di proporzionalità e collaborazione istituzionale.

Gli audit saranno programmati con congruo preavviso, non inferiore a 15 (quindici) giorni lavorativi, salvo i casi di urgenza connessi a incidenti di sicurezza, sospette violazioni, segnalazioni dell'Autorità competente o situazioni che possano compromettere la

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

continuità operativa o la sicurezza dell'infrastruttura regionale, nei quali casi il precedente termine potrà essere ridotto.

18. CLAUSOLA DI MANLEVA

L'Utente manleva e tiene indenne la Regione da qualsiasi pretesa, sanzione (incluse quelle del Garante Privacy), azione o richiesta di risarcimento avanzata da terzi (incluso il proprio Fornitore) derivante dall'uso illecito, negligente o imperito dei Servizi, dalla violazione di diritti di proprietà intellettuale o dalla perdita di dati imputabile a negligenza nella gestione delle risorse di competenza dell'Utente. L'Utente dovrà sostenere tutti i costi, risarcimenti di danni e oneri, incluse le eventuali spese legali, che dovessero derivare da queste richieste e si impegna ad informare la Regione Basilicata se tali richieste siano avanzate nei suoi confronti.

L'Utente esonera la Regione Basilicata da responsabilità per i danni derivanti da ritardi, cattivo funzionamento, sospensione o interruzione nell'erogazione dei Servizi che siano stati causati da:

- caso fortuito e forza maggiore (ad esempio, sismi, alluvioni, frane, smottamenti e più in genere eventi naturali avversi, crolli di edifici, incendi, epidemie, restrizioni alla mobilità imposte a livello locale o nazionale, atti di violenza e terrorismo, scioperi, carenza di componenti necessarie per erogare i Servizi ecc.);
- inadempienze o errori dell'Utente e/o del Fornitore (ad es. presenza di bug applicativi o mancato aggiornamento dei sistemi di competenza dell'Utente, mancato rinnovo di licenze a carico dell'Utente etc.);
- malfunzionamenti o non conformità degli apparecchi usati dall'Utente e/o dal Fornitore per usufruire dei Servizi e che non siano stati forniti dalla Regione Basilicata;
- manomissione o interventi sui Servizi eseguiti dall'Utente, dal suo Fornitore o da soggetti terzi non autorizzati dalla Regione Basilicata;
- eventi non prevedibili o non evitabili dalla Regione Basilicata con l'ordinaria diligenza.

Con riferimento alle attività di monitoraggio continuo, Vulnerability Assessment (VA) e Penetration Test (PT) svolte dalla Regione o da soggetti da essa incaricati e finalizzate a garantire un livello adeguato di sicurezza (NIS2, art. 32 GDPR), l'Utente esonera la Regione da responsabilità per eventuali malfunzionamenti, rallentamenti, crash di sistema, riavvii forzati, perdita o corruzione di dati, indisponibilità temporanea dei Servizi, alterazioni di configurazioni, interruzioni operative, danni indiretti o consequenziali,

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

derivanti da eventi intrinseci alle attività di verifica, non ragionevolmente evitabili pur in presenza di diligenza professionale e di adeguate misure tecniche e organizzative, fatti salvi i casi di dolo o colpa grave direttamente imputabili alla Regione.

L'Utente si impegna a manlevare e tenere indenne la Regione Basilicata da pretese, azioni o richieste di terzi connesse alle attività svolte conformemente al presente atto, nei limiti di cui all'art. 1229 c.c.. Resta in ogni caso esclusa qualsiasi esenzione di responsabilità per dolo, colpa grave, violazione delle misure di sicurezza concordate o svolgimento di attività eccedenti il perimetro autorizzato.

19. RISERVATEZZA

Sono ritenute confidenziali tutte le informazioni, i dati e la documentazione di natura tecnica, organizzativa, amministrativa o di sicurezza, comunque comunicati o messi a disposizione tra le Parti nell'ambito della fruizione dei Servizi e non destinati alla diffusione pubblica, ivi inclusi, a titolo esemplificativo e non esaustivo, informazioni relative all'architettura dei sistemi informativi, alle infrastrutture tecnologiche, alle configurazioni di sicurezza, al codice sorgente, ai programmi informatici, agli algoritmi, alle procedure operative, alla documentazione tecnica e ad ogni altro elemento informativo la cui divulgazione possa pregiudicare la sicurezza, l'integrità o il corretto funzionamento dei servizi erogati.

Gli obblighi di riservatezza di cui al presente articolo permarranno anche successivamente all'estinzione del rapporto contrattuale tra le Parti.

Resta ferma la facoltà di comunicare tali informazioni nei casi previsti dalla legge o su richiesta dell'Autorità giudiziaria o di altre Autorità pubbliche competenti, nonché nei casi previsti dalla normativa in materia di trasparenza amministrativa e accesso agli atti, dandone comunicazione all'altra Parte ove ciò sia consentito.

In caso di diffusione o utilizzo non autorizzato delle informazioni confidenziali, la Regione Basilicata si riserva di adottare ogni opportuna iniziativa a tutela dei propri diritti e interessi, nelle sedi competenti.

20. SOSPENSIONE E INTERRUZIONE DEL SERVIZIO

La Regione si riserva il diritto di sospendere o interrompere l'erogazione dei Servizi, ovvero di inibirne l'accesso da Internet, in caso di violazione da parte dell'Utente dei termini, delle condizioni e/o degli obblighi previsti dalla convenzione, dal presente documento e/o da quelli ivi richiamati. In tali casi, la Regione invierà all'Utente una formale comunicazione con la quale sarà richiesto di porre rimedio alla violazione entro

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

il termine massimo di 30 (trenta) giorni dal ricevimento della stessa. Decorso inutilmente tale termine, la Regione provvederà all'invio di una formale lettera di diffida e messa in mora, assegnando all'Utente un ulteriore termine massimo di 30 (trenta) giorni per provvedere all'adempimento e conformarsi agli obblighi previsti. Durante tale periodo, la Regione si riserva la facoltà di adottare gli interventi tecnici e organizzativi ritenuti necessari al fine di evitare la compromissione dell'infrastruttura regionale e dei Servizi erogati, ivi compresa, a titolo esemplificativo e non esaustivo, la sospensione totale o parziale del servizio o la limitazione dell'accesso ai medesimi. Decorso inutilmente anche l'ulteriore termine assegnato con la diffida e messa in mora, la Regione potrà procedere alla definitiva cessazione del servizio, come previsto al successivo art. 21.

La Regione Basilicata si riserva inoltre il diritto di sospendere o interrompere l'erogazione dei Servizi, ovvero inibirne l'accesso da Internet, senza preavviso nel caso in cui:

- si verifichino casi di forza maggiore o circostanze che, sulla base di una valutazione motivata della Regione, rendano necessario effettuare interventi urgenti o di emergenza, anche per la risoluzione di problemi di sicurezza o di situazioni che possano comportare rischio per l'integrità dell'infrastruttura di rete o per persone o cose. In tali casi i Servizi saranno ripristinati non appena cessate le cause che ne avevano determinato la sospensione;
- l'Utente utilizzi apparecchiature o, nel caso di Servizi IaaS, installi software malevoli, non verificati, privi di licenza (ove prevista), non autorizzati o comunque idonei a compromettere l'integrità, la sicurezza o la stabilità dell'infrastruttura IT;
- l'Utente risulti coinvolto, a qualsiasi titolo, in controversie giudiziali o stragiudiziali aventi ad oggetto atti o comportamenti posti in essere mediante l'utilizzo dei Servizi, ovvero su richiesta dell'Autorità Giudiziaria o di Pubblica Sicurezza;
- sussistano fondati motivi per ritenere che i Servizi siano utilizzati o acceduti da soggetti terzi non autorizzati.

In tali casi, la Regione darà comunicazione motivata all'Utente nel più breve tempo possibile. Resta fermo il diritto dell'Utente a richiedere una copia backup dei propri dati.

In generale, qualora vengano rilevate vulnerabilità di sicurezza relative ai software installati sull'infrastruttura regionale dall'Utente o su sua richiesta, la Regione potrà adottare misure tecniche di mitigazione o contenimento del rischio. I tempi di risoluzione richiesti all'Utente sono determinati in funzione del livello di gravità della vulnerabilità, classificato secondo lo standard CVSS (Common Vulnerability Scoring System) e pubblicato nel National Vulnerability Database (NVD).

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

Livello di gravità vulnerabilità (CVSS)	Intervallo punteggio (NVD)	Possibili azioni sul Servizio (Regione)	Tempo massimo di intervento (Utente)
Low	0.1 – 3.9	Nessuna azione immediata	30 giorni
Medium	4.0 – 6.9	Isolamento o sospensione del Servizio	10 giorni
High	7.0 – 8.9	Isolamento o sospensione del Servizio	3 giorni
Critical	9.0 – 10.0	Isolamento o interruzione immediata del Servizio	1 giorno

Si precisa che la presenza di software o sistemi operativi non più supportati dal produttore è considerata, ai fini della gestione del rischio, una vulnerabilità di gravità almeno "High".

Qualora non sia possibile procedere alla risoluzione definitiva della vulnerabilità per indisponibilità di aggiornamenti di sicurezza o per vincoli tecnici documentati, l'Utente è comunque tenuto ad adottare, entro i termini sopra indicati, idonee misure di mitigazione o compensative del rischio, ivi comprese quelle suggerite dal produttore del software interessato o individuate dalla Regione, fino alla disponibilità della soluzione definitiva. Qualora tale soluzione non venga resa disponibile dal produttore o dal Fornitore ovvero il software interessato raggiunga la condizione di fine supporto (End of Support), l'Utente è tenuto a provvedere, entro tempi congrui concordati con la Regione, alla sostituzione o all'aggiornamento del software con soluzioni supportate e conformi ai requisiti di sicurezza.

Le tempistiche sopra indicate sono definite sulla base delle buone pratiche internazionali in materia di vulnerability management e patch management (ISO/IEC 27001, ISO/IEC 27002 e NIST SP 800-40) e in coerenza con il principio di gestione del rischio previsto dalla Direttiva NIS2.

Resta ferma la facoltà della Regione Basilicata, qualora una vulnerabilità di sicurezza rappresenti un rischio per l'integrità, la disponibilità o la sicurezza dell'infrastruttura regionale o dei Servizi erogati ad altri Utenti, di adottare in via cautelativa le misure tecniche di contenimento ritenute necessarie, anche mediante limitazione dell'accessibilità al Servizio, isolamento delle risorse interessate o sospensione

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)
0971 668335
dg.transizionedigitale@cert.regione.basilicata.it

temporanea del Servizio. Tali interventi saranno comunicati all'Utente nel più breve tempo possibile e saranno limitati al tempo strettamente necessario alla risoluzione della vulnerabilità o all'adozione di adeguate misure di mitigazione.

Qualsiasi inadempimento o comportamento dell'Utente in contrasto con le presenti condizioni di utilizzo o con le disposizioni contenute nei documenti in esse richiamate non potrà essere interpretato come modifica, deroga o accettazione tacita delle stesse, anche in caso di mancata contestazione da parte della Regione Basilicata. L'eventuale mancato esercizio o ritardo da parte della Regione Basilicata nel far valere qualsiasi diritto non potrà in alcun modo essere interpretato come rinuncia a tali diritti o disposizioni.

21. CESSAZIONE DEL SERVIZIO

In caso di dismissione di un Servizio per qualunque causa, ivi compresa la migrazione verso altro provider, l'Utente ha diritto, ove applicabile, a richiedere la consegna su un proprio supporto fisico del backup completo dei propri dati e applicazioni, con verifica dell'integrità degli stessi, entro un periodo massimo di 30 giorni dalla data di comunicazione della dismissione, salvo diverso accordo tra le Parti. Decorso tale termine, la Regione provvederà alla disattivazione del Servizio ed alla cancellazione sicura e definitiva di tutti i dati. Resta espressamente esclusa qualsiasi responsabilità della Regione in relazione alla dismissione del Servizio e alla cancellazione dei dati effettuata conformemente alla procedura sopra descritta. Informazioni tecniche aggregate e anonimizzate, non riconducibili a dati personali o a specifici asset dell'Utente, potranno essere conservate esclusivamente per finalità di miglioramento della sicurezza e dell'efficienza dei Servizi.

Letto, confermato e sottoscritto digitalmente.

Lì, ……

L'Utente

……