



COMUNE DI S. STEFANO DI CAMASTRA
Provincia di Messina



COPIA DELIBERAZIONE DELLA GIUNTA COMUNALE

N. 64 della deliberazione

del 25.03.2025

OGGETTO: Approvazione del Regolamento per la Sicurezza della Informazioni e del Modulo di implementazione delle misure minime di sicurezza (MMS).

L'anno duemilaventicinque il giorno venticinque del mese di marzo alle ore 18,20 e seguenti, nella Casa Comunale e nella consueta sala delle adunanze, a seguito di regolare convocazione, si è riunita la Giunta Comunale, sono presenti:

N.	COGNOME E NOME	CARICA	PRESENTI	ASSENTI
1	Re Francesco	Sindaco	X	
2	Rampulla Santo	Vice Sindaco	X	
3	Amoroso Alessandro	Assessore	X	
4	Pellegrino Agostino	Assessore		X
5	Torcivia Rita Antonina	Assessore		X

Partecipa il Segretario Generale Dott.ssa Anna Angela Testagrossa.

Il Presidente, constatato che il numero dei presenti è legale, dichiara aperta la seduta e invita i presenti a deliberare sull'argomento in oggetto specificato.

LA GIUNTA COMUNALE

VISTA la legge 8 giugno 1990, n° 142, come recepita con L. r. 11 dicembre 1991, n° 48;

VISTA la L.r. 3 dicembre 1991, n° 44;

VISTA la L.r. 5 luglio 1997, n° 23;

CONSIDERATO che sulla proposta della presente deliberazione ha espresso **parere favorevole** il **Responsabile del servizio interessato, per quanto concerne la regolarità tecnica;**

VISTO il **parere favorevole del Responsabile dell'Area Economico Finanziaria, per quanto concerne la regolarità contabile,** ai sensi dell'art. 53 della legge 8 giugno 1990, n° 142, come recepito con l'art. 1, comma 1, lettera i), della l.r. 48/91 modificato dall'art. 12 della l.r. n° 30 del 23.12.2000;

VISTA la proposta di deliberazione concernente l'oggetto, predisposta **dall'Area Sviluppo Territoriale e Grandi Opere – Innovazione Tecnologica,** su indicazione **del Sindaco,** allegata alla presente per farne parte integrante e sostanziale;

PRESO ATTO dei presupposti di fatto e di diritto posti a base della proposta;

CONDIVISI i motivi che determinano l'emanazione dell'atto e i fini che si intendono perseguire;

CONSIDERATA la proposta che precede meritevole di approvazione in quanto diretta a soddisfare gli interessi di questo Ente;

VISTO l'Ordinamento EE.LL. vigente in Sicilia;

CON VOTI favorevoli unanimi espressi nei modi e termini di legge;

DELIBERA

Di approvare e fare propria l'allegata proposta di deliberazione che si intende integralmente trascritta ad ogni effetto di legge nel presente dispositivo sia per la parte relativa ai presupposti di fatto e di diritto che per la motivazione e per la parte dispositiva.

Successivamente

Ad unanimità di voti espressi nelle forme di legge.

DELIBERA

Dichiarare il presente provvedimento immediatamente esecutivo.

COMUNE DI SANTO STEFANO DI CAMASTRA
PROVINCIA di Messina
PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

PROPONENTE: SINDACO

OGGETTO: Approvazione del *Regolamento per la Sicurezza della Informazioni* e del *Modulo di implementazione delle misure minime di sicurezza (MMS)*.

PREMESSO che il Comune di Santo Stefano di Camastra dispone di una rete informatica e telematica, costituita da un insieme di strumenti e mezzi informatici quali le componenti *hardware* e *software* (*personal computer, tablet, server*; strumenti per la stampa e la riproduzione, programmi ecc.) e dei necessari collegamenti telematici per veicolare le informazioni da e verso le banche dati comunali;

ATTESO che l'utilizzo della rete informatica e telematica, di internet e della posta elettronica sono ormai indispensabili per perseguire con efficienza, efficacia ed economicità le funzioni istituzionali e gestionali dell'Ente come imposto dalle normative vigenti;

CONSIDERATO che:

- è compito del Comune assicurare la piena funzionalità del sistema informatico e promuovere ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati;
- risulta fondamentale individuare il complesso delle misure che configurano il livello minimo di protezione del sistema informatico comunale e del patrimonio informativo digitale dell'Ente;
- per dare attuazione a tali esigenze è necessario definire le regole per mitigare i rischi per la sicurezza delle informazioni nonché per assicurare un corretto utilizzo degli strumenti informatici messi a disposizione da parte del Comune, fornendo agli utenti (amministratori, responsabili di settore, dipendenti e collaboratori) specifiche disposizioni circa le modalità da seguire per un corretto utilizzo degli strumenti e delle risorse informatiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali, in modo da consentire a ciascun utente di collaborare attivamente alle politiche di sicurezza poste in atto dall'Amministrazione;
- è altresì necessario disciplinare le misure con le quali il Comune può eventualmente accertare e inibire le condotte illecite sull'utilizzo delle predette risorse, ponendo in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti informatici: il tutto senza invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità, come sancito dallo Statuto dei Lavoratori (L. 20 maggio 1970 n. 300 e ss.mm.ii.);
- ogni utente è responsabile del corretto utilizzo delle risorse informatiche, dei servizi a cui ha accesso e dei dati trattati a fini istituzionali;

CONSIDERATO altresì che

- è stato avviato il progetto FAST "Ambito A: verso la transizione digitale locale" al fine di supportare i piccoli comuni nel processo di innovazione e trasformazione digitale, in linea con quanto indicato nel Piano Nazionale di Ripresa e Resilienza, nel Piano strategico per la transizione digitale e la connettività "Italia digitale 2026" e nel Piano Triennale per l'Informatica;
- il progetto di cui sopra, gestito da Formez PA si rivolge a 285 Comuni con meno di 5.000 abitanti, tra i quali questo Comune, selezionati con una Manifestazione di interesse;
- nell'ambito del progetto "FAST PICCOLI COMUNI – Ambito A – Verso la transizione digitale locale", è stato avviato specifico progetto ed eseguite le seguenti fasi:
 - è stato realizzato l'assessment digitale evidenziando le aree di criticità e i possibili microprogetti realizzabili, tra i quali è stata data priorità al progetto relativo alle "Misure Minime di Sicurezza e Regolamento per la sicurezza informatica";
 - è stato realizzato il piano di lavoro ed avviati i lavori in data 22/04/2024;
- le attività sono state realizzate per fasi come di seguito indicato:
 - esame della bozza di regolamento per la sicurezza delle informazioni
 - esame e confronto sul Modello di implementazione delle MMS;
 - redazione di massima del Modulo MMS e del regolamento per la sicurezza delle informazioni;
 - confronto con l'Amministratore di sistema in merito agli elaborati in argomento al fine di definire gli aspetti tecnici di maggiore dettaglio;
 - validazione del MMS e del Regolamento per la sicurezza delle informazioni;
- il personale coinvolto nel progetto è stato il seguente:

- Responsabile Transizione digitale di questo Ente;
- Responsabile del servizio informatico di questo Ente;
- Professionista incaricato da questo Ente per svolgere le funzioni di Amministratore di sistema;
- Task Force di Fornez PA;

DATO ATTO che, espletate le varie attività, è stato elaborato, a cura del Responsabile per la transizione al digitale (RTD), nominato con Determina Sindacale n. 05 del 28/01/2021, uno specifico *“Regolamento per la Sicurezza della Informazioni”* costituito da n. 16 articoli più un glossario ed allegato al presente provvedimento per farne parte integrante e sostanziale;

RITENUTO che:

- tale regolamento tiene conto delle valutazioni effettuate tanto della figura nominata RTD, quanto dei Responsabili delle Aree funzionali dell’Ente;
- lo stesso appare conforme alle indicazioni del Garante per la Protezione dei dati personali, nonché alle altre disposizioni normative in materia;
- le prescrizioni di cui al Regolamento in parola si aggiungono ed integrano le specifiche istruzioni da fornire a tutti gli incaricati in attuazione del Regolamento Europeo 679/16 “General Data Protection Regulation” (d’ora in avanti Reg. 679/16 o GDPR);

AVUTO RIGUARDO:

- al Codice dell’Amministrazione Digitale, istituito con il decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii., che riunisce e organizza le norme riguardanti l’informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese;
- alla circolare AGID 2/2017 del 18 aprile 2017 e ss.mm.ii., con la quale sono state fornite indicazioni operative per la verifica delle condizioni minime di sicurezza ICT e del trattamento dei dati;

VISTI:

- il D.Lgs. n.165/2001 e il D.Lgs. 267/2000 e le loro ss.mm.ii.;
- il vigente statuto comunale;

EVIDENZIATO che il regolamento qui in trattazione costituisce integrazione operativa del vigente Regolamento Comunale sull’Ordinamento degli Uffici e dei Servizi;

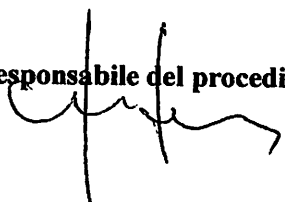
RICONOSCIUTA la propria competenza alla luce delle vigenti disposizioni normative, statutarie e regolamentari;

RAVVISATA l’opportunità, in sintonia con la proposta tecnica avanzata dagli Uffici, di procedere alla approvazione della presente proposta di deliberazione per le finalità in oggetto;

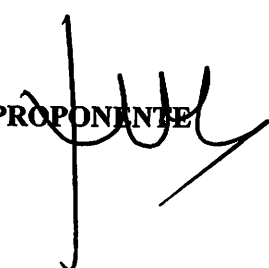
SI PROPONE che la GIUNTA COMUNALE DELIBERI

1. **di approvare** le premesse narrative e motivazionali al presente dispositivo, ritenendole qui integralmente trasposte;
2. **di dare atto** che in data 28/06/2024 sono state ultimate le attività e si è provveduto alla validazione del MMS e del Regolamento per la sicurezza delle informazioni;
3. **di approvare** il *“Regolamento Comunale per la Sicurezza della Informazioni”* allegato alla presente come parte integrante e sostanziale e costituito da n. 16 articoli più il glossario;
4. **di approvare** il *Modulo di implementazione delle misure minime di sicurezza (MMS)*, Circolare Agid 18/04/2017 n. 2;
5. **di specificare** che lo stesso regolamento costituisce integrazione operativa del vigente Regolamento Comunale sull’Ordinamento degli Uffici e dei Servizi;
6. **di impartire** indirizzo all’Ufficio Personale affinché copia del regolamento approvato sia consegnato e fatto sottoscrivere ai nuovi assunti, contestualmente alla sottoscrizione del contratto di lavoro;
7. **di incaricare** il Responsabile alla Transizione al Digitale dell’Ente in ordine a tutti gli adempimenti connessi e conseguenziali al presente deliberato con particolare riguardo:
 - ✓ alla pubblicazione del Regolamento in parola nel sito istituzionale dell’Ente nella sezione Amministrazione Trasparente – Atti generali;
 - ✓ alla sua diffusione presso i dipendenti allo scopo di garantire la massima adesione alle sue prescrizioni;
8. **di dichiarare**, infine con successiva e parimenti unanime votazione la presente deliberazione immediatamente eseguibile ai sensi dell’art. 134, comma 4, del d.lgs.vo n. 267/2000 e ss.mm. e ii. riconosciuta l’esigenza di assicurare il sollecito dispiegamento delle sue finalità.

Il responsabile del procedimento



IL PROPONENTE



COMUNE di SANTO STEFANO DI CAMASTRA

PARERI PREVENTIVI

ai sensi dell'art.53 della Legge 8 Giugno 1990, n° 142 recepito dalla L.R. 11 Dicembre 1991, n°48 e s.m.i.
e attestazione della copertura finanziaria

SULLA PROPOSTA DI DELIBERAZIONE DI GIUNTA COMUNALE N° 07/A.S. DEL 13/03/2025

OGGETTO: Approvazione del Regolamento per la Sicurezza della Informazioni e MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA (MMS)-

Il sottoscritto Dott. Ing. Danilo Di Mauro, Responsabile dell'Area Sviluppo Territoriale e Grandi Opere – Innovazione Tecnologica, esprime parere **FAVOREVOLE**, in ordine alla regolarità tecnica e alla correttezza amministrativa e attesta, ai sensi dell'art. 183 comma 8 del D.Lgs n° 267/2000, la compatibilità con i relativi stanziamenti di cassa e con le regole del patto di stabilità interno.

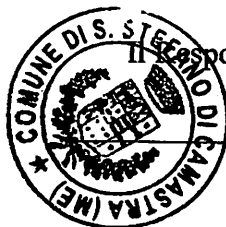
Data, 14/03/2025



Il Responsabile dell'Area
Dott. Ing. Danilo Di Mauro

La sottoscritta Rag. Rosa Celsa, Responsabile dell'Area Economico-Finanziaria, ai sensi del regolamento comunale sui controlli interni, **ATTESTA**, che l'approvazione del presente provvedimento, **non comporta** riflessi diretti sulla situazione economico finanziaria o sul patrimonio dell'Ente.
Per quanto concerne la regolarità contabile esprime parere **FAVOREVOLE**.

Data, 18-03-2025



Il Responsabile dell'Area Economico Finanziaria
Rag. Rosa Celsa



COMUNE di SANTO STEFANO DI CAMASTRA

CITTA' METROPOLITANA DI MESSINA
ADERENTE ALL'ENTE PARCO DEI NEBRODI
COMUNE D'EUROPA

AREA funzionale

SVILUPPO TERRITORIALE E GRANDI OPERE – INNOVAZIONE TECNOLOGICA

Servizio 1 – Pianificazione e Gestione Grandi Opere

REGOLAMENTO COMUNALE PER LA SICUREZZA DELLE INFORMAZIONI

<i>Tipo documento</i>	Regolamento
<i>Oggetto</i>	Sicurezza delle Informazioni

IL RESPONSABILE TRANSIZIONE DIGITALE
(Dott. Ing. Danilo Di Mauro)



DI MAURO
Danilo
14.03.2025
12:36:16
GMT+01:00

Indice

Articolo 1 – Oggetto e Scopo	3
Articolo 2 - Riferimenti normativi	3
Articolo 3 – Gli archivi cartacei – “scrivania pulita”	4
Articolo 4 - Utilizzo delle credenziali informatiche	4
Articolo 5 - Utilizzo del personal computer	6
Articolo 6 - Utilizzo di strumenti privati	6
Articolo 7 - Salvataggio dei dati, utilizzo supporti rimovibili	7
Articolo 8 - Utilizzo di altri dispositivi, stampanti e materiali di consumo	7
Articolo 9 - Protezione antivirus e anti-malware	7
Articolo 10 – Posta elettronica	8
Articolo 11 - Navigazione Internet	9
Articolo 12 - Controlli e monitoraggio	10
Articolo 13 - Controllo accessi fisici	11
Articolo 14 – L’Amministratore di Sistema	11
Art. 15 – Dismissione apparecchiature informatiche	12
Art. 16 – Aggiornamento delle disposizioni e delle regole tecniche	12
Glossario	13

Articolo 1 – Oggetto e Scopo

1) Il presente Regolamento:

- definisce le regole (compiti e responsabilità di tutto il personale) previste per mitigare i rischi per la sicurezza delle informazioni nonché per assicurare un corretto utilizzo degli strumenti informatici messi a disposizione da parte del Comune;
 - definisce le modalità per il corretto utilizzo degli strumenti ICT resi disponibili dal comune.
- 2) Nel documento vengono definite le modalità per il corretto trattamento delle informazioni contenute su supporto cartaceo ovvero gestite con strumenti elettronici, in particolare il PC e i cellulari. Tali informazioni devono essere sempre trattate in modo da garantirne la riservatezza, l'integrità e la disponibilità, e quando esse riguardano dati personali, i trattamenti devono tener conto della normativa in materia di protezione dei dati personali.
- 3) Questo regolamento deve essere osservato da tutti i dipendenti e amministratori, senza distinzione di ruolo e/o livello, nonché da tutti i collaboratori del comune, a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, ecc.).
- 4) Il mancato rispetto o la violazione delle norme contenute nella presente istruzione potrebbe comportare dei provvedimenti disciplinari e/o azioni giudiziarie previste dalle leggi vigenti.
- 5) Si precisa che la presente istruzione è integrativa di quanto previsto da:
- informative in materia di trattamento dei dati personali rilasciate ai dipendenti ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali;
 - lettere di incarico e designazioni destinate a responsabili e incaricati e le relative istruzioni ivi contenute, così come qualsiasi altra prescrizione in materia di privacy.

Articolo 2 - Riferimenti normativi

1. L'attività si realizza in conformità alle seguenti disposizioni normative:

- Decreto Presidente della Repubblica 13 giugno 2023, n. 81, Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165»
- Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (aggiornata 25.06.2009)
- Direttiva del Ministero per la pubblica amministrazione e l'innovazione 26 novembre 2009, n. 8; – Decreto legislativo 7 marzo 2005, n. 82, “Codice dell'amministrazione digitale” (e successive modificazioni e integrazioni);
- Legge 7 giugno 2000, n. 150, recante “Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni”.

- Linee guida per i siti web della PA, pubblicate dal Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica (ed. 2011 e smi)
- Decreto legislativo 18 agosto 2000, n. 267. Testo unico delle leggi sull'ordinamento degli enti locali a norma dell'articolo 31 della legge 3 agosto 1999, n. 265
- Legge 7 agosto 1990, n. 241 Nuove norme sul procedimento amministrativo.

Articolo 3 – Gli archivi cartacei – “scrivania pulita”

1. Le informazioni riservate e contenute su supporto cartaceo devono essere custodite e trattate, mediante l'adozione di idonee e preventive misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta. Al termine del lavoro o durante lunghe pause, sulle scrivanie non deve essere lasciata alcuna documentazione riservata (nel senso che contiene dati personali sensibile, ecc.) cartacea o su supporti rimovibili.
2. A tal fine si devono utilizzare contenitori (armadi, schedari eccetera) oppure le stesse stanze ove la documentazione è riposta (da interpretarsi estensivamente quali “contenitori”), purché muniti di serratura tale da consentire un'effettiva selezione degli accessi a favore dei soli soggetti incaricati.
3. Non lasciare accessibile la postazione di lavoro durante la propria assenza: bloccarla, prevedendo lo sblocco con password e attivare comunque un screen-saver automatico protetto da password che pulisca la videata entro alcuni minuti in caso di inutilizzo.
4. Sullo schermo della postazione, anche durante lo svolgimento della propria attività non devono essere facilmente visibili o accessibili informazioni riservate inutili per la corrente sessione di lavoro (ad esempio: lasciare aperto inutilmente un documento contenente informazioni sensibili, che possono essere inopportunamente lette da terzi durante o alla ripresa della sessione).

Articolo 4 - Utilizzo delle credenziali informatiche

1. Le credenziali di autenticazione per l'accesso ai sistemi e alla rete informatica sono costituite da un codice identificativo personale (username o user id) e da una parola chiave segreta (password) che dovrà essere custodita dall'utente con la massima diligenza e non divulgata, e che dovrà essere cambiata dall'utente al primo utilizzo, e successivamente almeno ogni sei mesi, oppure ogni tre mesi in caso di trattamento di dati sensibili e di dati giudiziari. La password deve essere costituita da almeno otto caratteri costituiti da lettere (maiuscole e/o minuscole), numeri e caratteri speciali, evitando parole di senso compiuto facilmente individuabili.
2. Le username o userid non hanno scadenza, se non alla cessazione del rapporto di lavoro. In caso di furto delle credenziali l'utente è tenuto a segnalarlo tempestivamente al Data Protection Officer, al proprio responsabile e al RTD; la rigenerazione delle credenziali è a cura del RTD. Al momento della cessazione del rapporto di lavoro, l'ufficio personale del comune segnala, via e-mail, al RTD la necessità di revocare le credenziali.
3. Si distinguono credenziali di accesso alla rete e di accesso ai programmi autorizzati, ciascuna con una specifica password, in particolare:
 - password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete;
 - password per l'accesso a particolari programmi e applicativi.

4. L'utente, in caso di prolungata e improvvisa assenza, può delegare un altro utente (c.d. fiduciario) all'accesso ai dati ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Dell'avvenuto conferimento della delega, l'utente delegante deve informare tempestivamente il Segretario comunale e il proprio responsabile d'ufficio. Di ciascun accesso dovrà essere redatto apposito verbale e informato l'utente delegante alla prima occasione utile. Nel caso in cui il dipendente non abbia delegato un suo fiduciario, il Responsabile dell'ufficio di appartenenza a cui il dipendente è assegnato può richiedere al RTD di disporre l'accesso alla postazione e/o alla casella di posta elettronica del dipendente assente da parte dell'Amministratore di sistema, in modo che si possa prendere visione delle informazioni e dei documenti per inderogabili necessità di svolgimento dell'attività lavorativa. Contestualmente, il RTD deve informare il dipendente dell'avvenuto accesso appena possibile fornendo adeguata spiegazione e redigendo apposito verbale.
5. In relazione alla necessità di limitarne gli accessi al solo personale specificamente autorizzato e di evitare l'uso improprio della rete informatica, il Responsabile dell'ufficio di competenza ha il dovere di segnalare al RTD la necessità di disattivare le credenziali di accesso ai sistemi o alla rete o alla casella di posta elettronica, precedentemente attribuite ad utenti su richiesta del medesimo Responsabile, qualora le motivazioni poste a base della richiesta venissero meno.
6. La sospensione delle credenziali avverrà d'ufficio qualora le stesse non vengano utilizzate per un periodo di sessanta giorni consecutivi.
7. L'accesso alle risorse della rete interna dall'esterno è consentito esclusivamente tramite un collegamento che necessita di autenticazione VPN (Virtual Private Network) ovvero solo gli utenti autorizzati vi possono accedere. L'abilitazione e le credenziali di accesso vengono forniti dal RTD, previa autorizzazione del Responsabile competente e con assunzione di responsabilità da parte del dipendente, ed unicamente tramite PC o laptop configurati ed installati secondo i profili definiti dal Comune e verificati dal RTD.
8. È assolutamente vietato fare accesso a qualsiasi sistema informatico con credenziali diverse da quelle assegnate.
9. Ogni utente è responsabile della corretta gestione della propria password, dei dispositivi di riconoscimento, delle informazioni per l'accesso ai sistemi e ai dati. Le credenziali sono personali e non cedibili, devono essere riconducibili al proprietario e devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi comunali sulla base del principio del "minimo privilegio".
10. Le password devono soddisfare i seguenti requisiti minimi:
- Non devono contenere il nome dell'account dell'utente o parti del nome completo dell'utente che superino due caratteri consecutivi
 - Devono avere almeno 8 caratteri di lunghezza
 - Devono contenere almeno tre delle seguenti quattro categorie:
 - Caratteri maiuscoli inglesi (dalla A alla Z)
 - Caratteri minuscoli inglesi (dalla a alla z)
 - Numeri (da 0 a 9)
 - Caratteri non alfabetici (ad esempio, !, \$, #, %)
 - Devono essere cambiate almeno ogni 180 giorni
 - Le vecchie password non possono essere riutilizzate prima di sei modifiche
11. Quando l'autenticazione a più fattori non è supportata, le utenze con ruolo amministratore devono utilizzare credenziali di elevata robustezza (e.g. almeno 14 caratteri). Le stesse utenze devono

inoltre sostituire le password con cadenza trimestrale.

12. Per un livello di sicurezza maggiore, è consigliabile per tutti gli utenti utilizzare un "pass phrase" anziché una password. Per "pass phrase" si intende una frase di senso compiuto, compreso spazi e segni ortografici. Tali frasi possono essere significative per l'utente e quindi facilmente ricordabili, ma risultano molto difficili da indovinare per i sistemi automatici. A puro titolo di esempio: "Il-mio-gatto-è-Silvestro"; "Mia-figlia-è-nata-il 21.05.2007"

Articolo 5 - Utilizzo del personal computer

1. Il Personal Computer, sia fisso che portatile, affidato al dipendente è uno strumento di lavoro; pertanto vi devono essere archiviati solo dati relativi all'attività svolta e non dati propri.
2. Le impostazioni dei PC e dei relativi programmi sono predisposte dal RTD sulla base di criteri e profili decisi dal comune in funzione della qualifica del dipendente e delle mansioni a cui questo è adibito. Il dipendente non può modificarle autonomamente; eventuali variazioni necessarie possono essere effettuate solo dal RTD.
3. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal RTD. Non è altresì consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
4. Solo il personale incaricato dal RTD è autorizzato a compiere interventi nel sistema informatico comunale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, installazione di programmi, manutenzione hardware etc.).
5. Non è consentita all'utente l'attivazione della password all'accensione del PC (BIOS), senza preventiva autorizzazione da parte del RTD.
6. I PC portatili devono essere collegati alla rete almeno ogni 15 giorni. In questo modo si garantisce che ricevano dai sistemi centrale gli aggiornamenti predisposti per tutte le postazioni client.

Articolo 6 - Utilizzo di strumenti privati

1. L'utilizzo di computer di proprietà di dipendenti, dirigenti, assessori, collaboratori, è consentito solo se questi siano dotati da software antivirus, approvato dal RTD, e regolarmente aggiornato.
2. L'utilizzo dei personal computer portatili deve seguire le stesse regole previste per i personal computer connessi in rete.
3. Ove possibile, i dischi dei PC portatili devono essere cifrati.
4. L'eventuale furto o smarrimento del pc portatile deve essere tempestivamente denunciato all'autorità competente con indicazione della marca, modello, numero seriale. Successivamente dovrà essere presentata copia della denuncia al RTD ed informato il Responsabile per la protezione dei dati personali ed il proprio Responsabile.
5. È vietato l'utilizzo di smartphone e tablet per connettersi dall'esterno alle applicazioni e dati del S.I comunale. Tali strumenti possono essere utilizzati per connettersi al sistema di posta elettronica.

Articolo 7 - Salvataggio dei dati, utilizzo supporti rimovibili

1. Nel rispetto dell'obbligo, previsto dall'art. 35 del D.L. 76/2020, di migrare i propri CED verso ambienti cloud, il Comune ha migrato (sta migrando) il software che compone il proprio Sistema Informativo in tale modalità. Eventuali applicativi legacy operanti in modalità diversa devono essere segnalati al RTD che procederà a individuare la modalità per il successivo passaggio al cloud o gestione del server.
2. La sicurezza e il salvataggio dei dati, nonché il regolare aggiornamento del software in Cloud è assicurato dai contratti stipulati con i vari fornitori.
3. I dischi e le altre unità di memorizzazione locali (es. disco C: del PC, pen drive) non sono soggetti al salvataggio automatico.
4. I supporti magnetici rimovibili (CD, DVD, pen drive, dischi fissi esterni, etc.) contenenti dati personali e/o informazioni di proprietà del Comune e/o di terzi, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, perso, distrutto o, successivamente alla normale cancellazione, recuperato da terzi. In ogni caso, i supporti magnetici devono essere custoditi sottochiave o, comunque, in luoghi non accessibili a terzi. È preferibile che i dati contenuti in questi dispositivi siano crittati.

Articolo 8 - Utilizzo di altri dispositivi, stampanti e materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente ai compiti di natura strettamente istituzionale.
2. Ciascun utente avrà cura di evitare sprechi o utilizzi inappropriati dei suddetti materiali. In particolare, per quanto riguarda le operazioni di stampa, verificherà previamente le impostazioni della stampante e il numero delle pagine da stampare, onde evitare stampe errate o superflue e prediligerà la stampa fronte-retro.
3. Il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici comunali di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen drive e supporti di memoria. In generale tutti i dispositivi elettronici comunali sono forniti al dipendente per lo svolgimento della sua attività lavorativa. L'uso per fini personali è da considerare pertanto eccezionale e limitato ad utilizzo occasionale e di breve durata.

Articolo 9 - Protezione antivirus e anti-malware

1. All'atto del collegamento in rete, il software antivirus sui singoli PC viene controllato ed eventualmente aggiornato da un server centrale gestito dal RTD; il software su tale server è aggiornato costantemente.
2. Il sistema informatico del Comune è protetto da apposito software anti-malware, aggiornato con la massima frequenza rispetto alle ultime tipologie di attacco scoperte, gestito tramite una console centralizzata che assicura la massima efficacia dell'azione di contrasto. Il SII configura ed attiva, nei personal computer assegnati al personale per la propria postazione di lavoro, i firewall locali; le relative regole di protezione sono definite, controllate e distribuite dal sistema centrale di gestione.
3. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico comunale mediante virus o mediante ogni altro software dannoso. Nel caso in cui il

software antivirus rilevi la presenza di un virus, l'utente deve immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al RTD.

4. Ogni dispositivo magnetico di provenienza esterna al comune deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso è rilevato un virus, deve essere prontamente catalogato come "fuori uso" e bonificato.

Articolo 10 – Posta elettronica

1. La posta elettronica è uno strumento fornito dal comune esclusivamente quale supporto all'attività lavorativa, ivi comprese le attività che siano strumentali e connesse alla stessa.
2. Poiché le caselle di posta sono di proprietà del Comune, che ne concede l'uso ai dipendenti secondo le norme indicate nella presente istruzione, i dipendenti assegnatari sono responsabili del corretto utilizzo delle stesse.
3. L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.
4. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.
5. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.
6. Le comunicazioni via posta elettronica devono avere un contenuto professionale, corretto e rispettoso a tutela della dignità delle persone e dell'immagine e reputazione del Comune. Le comunicazioni in uscita devono essere firmate inserendo sempre il proprio nome e cognome, servizio di appartenenza, "Comune" e recapito telefonico.
7. A ciascun utente, al momento dell'assunzione e/o attivazione del contratto, è assegnata una casella di posta elettronica. L'attivazione di una ulteriore casella di posta elettronica a supporto della funzione, per esempio di gruppo o di progetto, deve essere richiesta tramite il responsabile della struttura organizzativa.
8. In caso di assenza preventivata (ad es., per ferie o attività di lavoro fuori sede) gli utenti dovranno impostare il proprio sistema di Posta Elettronica in modo che possa inviare automaticamente, messaggi di risposta contenenti i riferimenti di un altro soggetto o altre utili modalità di contatto della struttura.
9. In caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta (anche avvalendosi di servizi webmail), il Titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema) l'attivazione di un analogo accorgimento, avvertendo gli interessati.
10. In previsione che in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il lavoratore dovrà delegare, anche preventivamente, un utente (c.d. fiduciario) a verificare il contenuto di messaggi e ad inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo

svolgimento dell'attività lavorativa. Il Fiduciario provvederà a verbalizzare tale attività e ad informare il lavoratore interessato alla prima occasione utile.

11. I messaggi di posta elettronica devono contenere un avvertimento ai destinatari nel quale sia dichiarata la natura non personale dei messaggi stessi, precisando: *“Messaggio riservato attinente all'attività del Comune di Santo Stefano di Camastra e contenente informazioni di natura professionale. Le eventuali risposte potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente. Se ricevuto per errore, o non delegati dal destinatario, Vi preghiamo di comunicarlo e di eliminarlo definitivamente”*.
12. Il personale è tenuto a non aprire allegati di posta contenuti in e-mail aventi mittente e/o oggetto sospetti; ciò al fine di prevenire danni causati da software nocivi (per es. virus, worm, spyware, ecc.) che potrebbero essere contenuti negli allegati delle e-mail stesse.
13. Al fine di prevenire spamming e phishing, si raccomanda di:
 - non rispondere mai a messaggi di presunto spamming, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;
 - non rispondere o inoltrare e-mail di c.d. “Catene di S. Antonio”, ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
 - non spedire un'e-mail a tutti i dipendenti del Comune; se proprio necessario, si deve utilizzare “:bcc” sia per rispettare la privacy sia per evitare che le eventuali risposte vadano anche esse a tutti i dipendenti;
 - prestare massima attenzione alle e-mail che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di fornitori di servizi, ecc.).
14. È vietato l'utilizzo dell'indirizzo e-mail comunale per l'iscrizione a qualsiasi servizio on line (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) che non sia strettamente correlato alla propria attività istituzionale.
15. La posta elettronica comunale può essere utilizzata da dispositivi personali (es. Tablet, cellulare, etc) solo tramite il servizio Webmail.

Articolo 11 - Navigazione Internet

1. L'accesso alla rete Internet è stato fornito al personale a beneficio della produttività dando la possibilità di usufruire delle risorse informative presenti nella rete. Il personale ha la responsabilità di utilizzare la rete Internet per finalità legittime e strettamente necessarie allo svolgimento delle mansioni lavorative.
2. Non è consentito ai dipendenti l'utilizzo di modem personali (es. hotspot o altri sistemi), o di qualunque altro dispositivo di navigazione del tipo “internet-Key” con account personali;
3. È espressamente vietato:
 - lo scarico di software gratuiti e shareware prelevati da siti internet, salvo casi espressamente autorizzati;
 - ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
 - la partecipazione, per motivi non professionali a Forum, l'utilizzo di Chat line; di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (nickname);

- la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica;
 - scaricare/scambiare materiale coperto da diritto d'autore (es. film, musica, ebook, etc.);
 - scaricare/scambiare materiale a contenuto pornografico o pedopornografico;
 - eseguire o favorire pratiche di Spamming.
4. È ammesso l'utilizzo di Internet per assolvere a proprie incombenze amministrative e burocratiche (ivi comprese le operazioni di remote Banking, acquisti on line e simili) senza allontanarsi dal luogo di lavoro. Tale modalità di utilizzo di Internet deve essere contenuta nei tempi strettamente necessari allo svolgimento delle transazioni e privilegiando, quando possibile, l'utilizzo delle pause di lavoro. Il fine è quello di contribuire a ridurre gli spostamenti delle persone e gli oneri logistici e di personale a carico dell'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi (par. 3 "Utilizzo della rete Internet" della Direttiva n. 2/2009 della Presidenza del Consiglio dei ministri, Dipartimento della funzione pubblica).

Articolo 12 - Controlli e monitoraggio

1. Il Comune si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e della presente istruzione.
2. Per esigenze organizzative, produttive e di sicurezza il Comune può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato e indiretto, relativo ad aree, settori o gruppi di utenti. Qualora – durante un controllo generalizzato – vengano rilevate anomalie nell'utilizzo degli strumenti informatici, il Comune procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente alla presente istruzione, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.
3. In nessun caso il Comune perseguirà finalità di controllo a distanza diretto, sistematico e/o intenzionale dell'attività dei lavoratori. In particolare, in linea con quanto previsto dalla Deliberazione n. 13/2007 del Garante per la protezione dei dati personali, non si procederà:
 - alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per lo svolgimento del servizio;
 - alla riproduzione e alla eventuale memorizzazione sistematica delle pagine web visualizzate;
 - alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
 - all'analisi occulta di computer affidati in uso.
4. I sistemi informativi sono verificati sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti interni, ed in particolare dei requisiti minimi di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali.
5. Le attività degli utenti possono essere registrate in files di LOG come di seguito indicato:

- log del firewall: tale raccolta viene attivata solo in caso di necessità per effettuare verifiche sul funzionamento della rete e poter identificare incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
 - log del server di posta: tali log vengono raccolti e conservati per poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
 - log del software applicativo del Sistema Informativo: tali log vengono raccolti e conservati per poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
 - log degli accessi degli amministratori di sistema ai sistemi amministrati: la raccolta e conservazione di tali log è motivata dalla necessità di ottemperare al Provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema.
6. L'accesso ai log ed ai contenuti dei sistemi di posta elettronica è permesso solo ed esclusivamente nei seguenti casi:
- Richiesta Autorità Giudiziaria;
 - Richiesta Pubblica Sicurezza;
 - Attività ispettive preventive e/o difensive (Organi di vigilanza);
 - Soluzione di incidenti informatici o telematici;
 - Esigenze di continuità operativa (recupero dati, assenze prolungate, etc.).
7. I tempi di conservazione previsti per le tipologie di log sopra elencate è fissato per un periodo semestrale. Ciò è motivato dalla necessità di utilizzare tali log per la verifica delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali relativi agli amministratori di sistema e di avere una policy di retention dei log adeguata a tutte le tipologie, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.
8. In caso di controlli preventivi (di effettivo rispetto di regole comunali) e per accesso dovuti ad esigenze di continuità, il lavoratore interessato dovrà essere preavvisato al fine di garantire la correttezza e la trasparenza verso il lavoratore per mezzo della preventiva informazione.
9. Per i controlli difensivi o richiesti da Pubbliche Autorità (PS, ecc.), ovvero in casi di incidenti che necessitino interventi immediati e urgenti, la preventiva informazione può essere omessa, in quanto può compromettere la difesa o l'accertamento di diritti o di responsabilità in giudizio o l'attività istituzionale dell'ente. Nel caso di incidenti di tal natura, l'informazione potrà/dovrà essere data a posteriori.
10. Nell'espletare controlli e verifiche, le funzioni preposte devono garantire la massima riservatezza dei dati conosciuti, anche incidentalmente, pena l'applicazione di sanzioni disciplinari in base alla gravità dell'accaduto. I dati potranno essere comunicati solo ed esclusivamente a soggetti interni o esterni del comune per cui la comunicazione sia dovuta in relazione alle finalità perseguite con l'accesso (per esempio, nei casi indicati al comma 3, alle Forze dell'Ordine, ad incaricati di funzioni comunali preposte alle azioni legali o alla soluzione dei problemi.

Articolo 13 - Controllo accessi fisici

1. Le indicazioni contenute nel presente capitolo mirano alla riduzione dei rischi derivanti dall'accesso di soggetti non autorizzati alla sede del Comune e ai locali tecnici.
2. I vani tecnici delle sedi sono deputati a rappresentare le aree sicure finalizzate a prevenire l'accesso fisico non autorizzato, danni e disturbi alle informazioni del Comune ed alle infrastrutture di elaborazione delle informazioni.
3. L'accesso ai suddetti vani è consentito unicamente al RTD o un suo delegato.

Articolo 14 – L'Amministratore di Sistema

1. L'amministratore di sistema è individuato con atto del Responsabile per la Transizione al Digitale (RTD).
2. L'accesso ai sistemi con privilegi amministrativi è consentito solo all'Amministratore di sistema e al Responsabile per la Transizione Digitale (o un loro delegato che abbia le competenze ed effettive necessità di modificare la configurazione dei sistemi).
3. L'atto di incarico dell'Amministratore di sistema deve indicare almeno le seguenti attività allo scopo di soddisfare quanto previsto dalle Misure Minime di Sicurezza dell'AGID:
 - a. Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato
 - b. Scrivere un documento, approvato del RTD, che indichi la configurazione standard e le policy di dominio con la quale tutte le postazioni PC vengono create e gestite utilizzando un'immagine standard. L'immagine standard è creata con l'obiettivo di limitare le azioni degli utenti che possano compromettere la propria postazione o la rete dell'ente. L'utente non può installare software, modificare configurazioni (es impostazioni dei browser installati, associazione delle estensioni), creare/modificare utenti e gruppi locali, modificare i permessi su file system ecc.
 - c. Predisporre e mantenere aggiornata la configurazione base da installare sui PC
 - d. Effettuare, con cadenza mensile, la procedura di monitoraggio e di vulnerability assessment, nonché l'aggiornamento del antivirus ogni volta venga rilasciata un aggiornamento del codice o della base dati
 - e. Verificare che le vulnerabilità emerse dalle scansioni dei software siano effettivamente sanate dopo l'installazione di patch o di azioni correttive che ne limitano il possibile rischio
 - f. Predisponga un documento in cui elencare quali apparati sono esposti a maggior rischio rispetto ad altri (es. per tipologia di servizio o per i tipi di dati trattati, ecc.) indicando precisamente il livello di rischio corrispondente (Alto, Medio e Basso). Per rischio si intende il tipo di criticità, che al verificarsi dell'evento malevolo, potrebbe influire gravemente sul funzionamento della struttura o di una sua parte.

Art. 15 – Dismissione apparecchiature informatiche

1. I settori dovranno procedere alla dismissione/smaltimento, delle apparecchiature informatiche e tecnologiche (PC, monitor, stampanti, ecc.) nella loro disponibilità per le quali sia intervenuta una dichiarazione di fuori uso o di obsolescenza da parte del RTD, secondo quanto previsto dalla normativa (GDPR, Rifiuti di apparecchiature elettriche ed elettroniche (Raee), ecc) e secondo le procedure previste dal servizio competente per la gestione del patrimonio dell'ente.
La dismissione e lo smaltimento dei dispositivi deve essere preceduta dall'eliminazione dei dati eventualmente memorizzati negli stessi.

Art. 16 – Aggiornamento delle disposizioni e delle regole tecniche

1. Le disposizioni generali contenute nel presente Regolamento possono essere soggette ad aggiornamenti, integrazioni e/o correzioni, in relazione all'evolversi della tecnologia, all'entrata in vigore di sopravvenute disposizioni di legge o all'evolversi delle esigenze dell'Amministrazione. Il Responsabile per la Transizione al Digitale (RTD) è incaricato di emanare ed aggiornare le regole tecniche necessarie per l'attuazione delle disposizioni di carattere generale contenute nel presente Regolamento.

Glossario

Access Point	<p>L'access point (AP) è un dispositivo di rete che, collegato ad una rete LAN (Local Area Network) tramite uno switch, un router o una presa di rete, costituisce il punto di unione tra una rete cablata e i dispositivi dotati di schede di rete senza fili o Wi-Fi</p> <p>Più AP possono collegarsi direttamente tra loro in "mesh" per costituire una rete Wi-Fi più estesa. I nodi di una rete mesh sono tutti accomunati dallo stesso SSID, un acronimo di "service set identifier", cioè il nome che identifica la nostra rete WiFi</p>
Account	<p>Creare o acquistare un account vuol dire fare una richiesta affinché vengano dati ad una persona le credenziali (es. user ID e password) con i quali l'utente può accedere ad un servizio. Gli esempi più noti sono:</p> <ul style="list-style-type: none">• l'account che si chiede ad un ISP per accedere ad Internet e alla posta elettronica• l'account che un amministratore di rete crea per fare in modo che un utente acceda al PC e ai servizi di rete
AGID	<p>E' l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica</p>
Amministratori di sistema	<p>Soggetti deputati a intervenire per garantire l'efficienza e la funzionalità di un determinato sistema informatico, aventi la possibilità di accedere a dati personali qualora l'accesso sia assolutamente necessario per raggiungere le finalità proprie del ruolo ricoperto</p>
Antivirus	<p>Programma in grado di riconoscere un virus presente in un file e di eliminarlo o di renderlo inoffensivo</p>
API	<p>Un insieme di procedure (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito</p>
Apparati attivi	<p>Apparecchiature hardware collegate alla rete che ne permettono il funzionamento (es. router, switch)</p>

Application Server	Server dedicato all'esecuzione di applicazioni alle quali fornisce servizi di tipo infrastrutturale. Nelle architetture software è il server in cui è localizzata la logica applicativa.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
Aree condivise	Spazi di memorizzazione messi a disposizione degli utenti sui sistemi centralizzati per la condivisione e lo scambio di files
Attachment	File allegato: può essere un allegato alla posta elettronica o a qualsiasi software di gestione dei file
Backbone	Una dorsale di rete o backbone, in ambito ICT, è un collegamento ad alta velocità di trasmissione e capacità tra due server o router di smistamento informazioni e appartenente normalmente alla rete di trasporto di una rete di telecomunicazioni. Una dorsale è una linea logica che può essere fisicamente singola o multipla con la quale vengono interconnessi ad un livello superiore (facendoli confluire) parti di rete con velocità e capacità inferiore grazie a meccanismi di moltiplicazione.
Backup	Procedura per la duplicazione dei dati su un supporto distinto da quello sul quale sono memorizzati, in modo da garantirne una copia di riserva
Banda	Quantità di dati per unità di tempo che può viaggiare su una connessione. Nella "banda ampia" la velocità varia da 64 Kbps a 1,544 Mbps. Nella "banda larga" la comunicazione avviene a velocità superiori a 1,544 Mbps
Bootstrap del pc	Indica, in generale, l'insieme dei processi che vengono eseguiti da un computer durante la fase di avvio, in particolare dall'accensione fino al completo caricamento in memoria primaria del kernel (nucleo) del sistema operativo a partire dalla memoria secondaria
CAD	Il Codice dell'Amministrazione Digitale è il testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato.
Client	In informatica, con client (in italiano detto anche cliente) si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al

Cloud Computing	<p>Il cloud computing (in italiano nuvola informatica) indica, in informatica, un paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita.</p> <p>Indica un paradigma di erogazione di servizi offerti on demand da un fornitore ad un cliente finale attraverso la rete Internet. Il cloud è un modello che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad es. reti, server, storage, applicazioni e servizi) che possono essere erogate come un servizio</p>
Comunicazioni Elettroniche	Scambio di informazioni tra due o più interlocutori che avvenga utilizzando mezzi di comunicazione basati su dispositivi elettronici quali ad esempio posta elettronica, sistemi di comunicazione istantanea, telefonia VoIP o cellulare
Cookie	Tradotto letteralmente significa biscotto. E' un file memorizzato sul proprio computer che identifica il computer quando è collegato ad alcuni siti Internet
CSP	Cloud Service Provider–Fornitori di servizi in cloud
Data breach	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
Database	In informatica, il termine database, tradotto in italiano con banca dati, base di dati (soprattutto in testi accademici) o anche base dati, indica un archivio di dati, riguardanti uno stesso argomento o più argomenti correlati tra loro,
DNS (Domain Name System)	Sistema che gestisce gli indirizzi dei domini Internet e Intranet traducendo una richiesta human-friendly – un nome di dominio come <u>www.comune.XXX.it</u> , PC_Utente1 – e lo traduce in un indirizzo IP , come 212.210.147.8
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare. testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Dominio (nome di dominio)	Un nome di dominio, in informatica, è costituito da una serie di stringhe separate da punti, che identifica il dominio dell'autonomia amministrativa, dell'autorità o del controllo all'interno di internet. I nomi di dominio sono formati dalle regole e dalle procedure del Domain Name System (DNS). Qualsiasi nome registrato nel DNS (ad esempio <u>comune.XXXXX.it</u>) è un nome di dominio. Essi vengono

	<p>utilizzati in diversi contesti di rete e in ambito specifico per la denominazione o l'indirizzamento.</p> <p>In generale, un nome di dominio rappresenta una risorsa Internet Protocol (IP), ad esempio un computer utilizzato per accedere a Internet (host), un server che ospita un sito web o il sito web stesso, oppure qualsiasi altro servizio comunicato tramite Internet. A differenza degli indirizzi IP, dove la parte più importante del numero è la prima partendo da sinistra, in un nome DNS la parte più importante è la prima partendo da destra: questa è detta dominio di primo livello (o TLD, Top Level Domain), per esempio ".it" o ".com".</p>
<p>Dominio Microsoft</p>	<p>Definizione di Microsoft: "un insieme di computer che condividono un database di risorse di rete e che vengono amministrati come un'unità con regole e procedure comuni"</p> <p>In termini molto semplici, un dominio è una rete di computer, LAN, MAN o WAN di un'organizzazione (ad esempio un'azienda o un ente pubblico o una scuola/università), ove la logica client-server è supportata, oltre che da connessioni fisiche e relativi protocolli (ad esempio il comune indirizzo IP), anche da regole (policy) di connessione logica di tipo autorizzativo (regole di sicurezza). In questo contesto, un client deve sottostare a procedure di autenticazione specifiche, definite da servizi che risiedono su un server. Queste procedure, che solitamente sottendono una gerarchia di profili (in termini di permessi e accessi alle risorse o ai sistemi), determinano l'appartenenza o meno al dominio, struttura di distribuzione e condivisione centralizzata.</p>
<p>Download</p>	<p>Il download, anche noto come "scaricamento", indica in informatica l'azione di ricevere o prelevare da una rete telematica (ad esempio da un sito web) un file, trasferendolo sul disco rigido del computer o su altra periferica dell'utente. Nella maggior parte dei casi, il download di un file è la conseguenza di una richiesta più o meno trasparente da parte di un utente del sistema; l'azione inversa è invece detta upload.</p>
<p>E-mail</p>	<p>La posta elettronica, in inglese e-mail (abbreviazione di electronic mail), è un servizio Intranet/Internet grazie al quale ogni utente abilitato può inviare e ricevere dei messaggi utilizzando un computer o altro dispositivo elettronico (come palmare, smartphone, tablet) connesso in rete attraverso un proprio account di posta registrato presso un fornitore del servizio</p>
<p>File</p>	<p>Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.</p>

File di log	File che registra attività di base, quali l'accesso ai dispositivi, e che è presente sui PC, server e dispositivi di rete
File server	In informatica, il termine file server si riferisce generalmente ad una macchina progettata per mettere a disposizione degli utilizzatori di una rete di computer dello spazio su un disco (disco singolo o composto da più dischi) nel quale sia possibile salvare, leggere, modificare, creare file e cartelle centralizzate, condivise da tutti oppure accessibili secondo regole o autorizzazioni generalmente assegnate dal gestore di rete organizza e gestisce. Tale macchina può essere un computer o un Network Attached Storage (NAS), cioè un apparecchio specificatamente studiato e costruito allo scopo. Per estensione il termine si riferisce anche al programma di tale macchina che si occupa di rendere disponibili i dati
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage
Firewall	Apparato di rete hardware o software che filtra tutto il traffico informatico in entrata e in uscita e che di fatto evidenzia un perimetro all'interno della rete informatica e contribuisce alla sicurezza della rete stessa. Apparato di protezione perimetrale della rete
Firma Digitale	Firma Digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Firma Elettronica	«firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare - articolo 3 del Regolamento eIDAS (Regolamento Europeo) vedi CAD (decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni)
Firma Elettronica Avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS (Regolamento Europeo) e CAD (decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni)
Firma Elettronica Qualificata	Vedi articoli 3 del Regolamento eIDAS (Regolamento Europeo) e CAD (decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni)

GDPR	Il Regolamento (UE) 2016/679 del Parlamento europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
Hardware	L'hardware, traducibile in italiano come componente fisico, materiale informatico o supporto fisico (sigla HW, dall'inglese hard «duro, pesante» e ware «merci, prodotti», su imitazione del termine software), è la parte materiale di un computer, ovvero tutte quelle parti elettroniche, elettriche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento; più in generale il termine si riferisce a qualsiasi componente fisico di una periferica o di una apparecchiatura elettronica, ivi comprese le strutture di rete; l'insieme di tali componenti è anche detto componentistica
Help Desk	In informatica e organizzazione aziendale l'help desk (termine mutuato dalla lingua inglese che letteralmente significa scrivania di aiuto ovvero supporto tecnico) è un servizio professionale aziendale, in buona parte orientato al problem solving, volto a fornire assistenza/supporto tecnico e/o informativo, all'utente/cliente, relativamente all'acquisto e/o utilizzo di prodotti elettronici o servizi informatici, con lo scopo dunque di fornire indicazioni o risolvere problemi su prodotti hardware come computer, apparecchiature elettroniche o software
ICT	Acronimo di "Information and Communications Technology", in italiano "Tecnologie dell'informazione e della Comunicazione" (in acronimo TIC), sono l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese).
Indirizzamento	Attività di assegnazione di indirizzi logici (es. indirizzo IP) ad apparati attivi
Integrità	La protezione contro la perdita, la modifica, la creazione o la replica non autorizzata delle informazioni ovvero la conferma che i dati trattati siano completi
Internet	Internet è una rete di telecomunicazioni ad accesso pubblico che connette vari dispositivi o terminali in tutto il mondo, rappresentando dalla sua nascita uno dei maggiori mezzi di comunicazione di massa (assieme a radio e televisione), grazie all'offerta all'utente di una vasta serie di contenuti potenzialmente informativi e di servizi. Si tratta di un'interconnessione globale tra reti di telecomunicazioni e informatiche di natura e di estensione diversa, resa possibile da una suite di protocolli di rete comune chiamata "TCP/IP" dal nome dei due protocolli principali, il TCP e l'IP, che costituiscono la "lingua" comune con cui i computer connessi a Internet (gli host) sono interconnessi e comunicano tra loro a un livello superiore

	<p>indipendentemente dalla loro sottostante architettura hardware e software, garantendo così l'interoperabilità tra sistemi e sottoreti fisiche diverse</p>
Interoperabilità	<p>Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi</p>
Intranet	<p>La Intranet è una rete locale (Local Area Network), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso alle informazioni. E' una rete aziendale privata completamente isolata dalla rete esterna (Internet) a livello di servizi offerti (es. tramite LAN), rimanendo dunque a solo uso interno, comunicando eventualmente con la rete esterna e altre reti attraverso opportuni sistemi di comunicazione (protocollo TCP/IP, estendendosi anche con collegamenti WAN e VPN) e relativa protezione (es. firewall).</p>
IP	<p>Indirizzo che permette di identificare in modo univoco un dispositivo (es. computer, Server, switch, router ecc) collegato in rete. Si suddivide in due parti, la prima individua la rete dove si trova il dispositivo, la seconda individua il dispositivo all'interno di quella rete</p>
IPSEC	<p>E' una collezione (insieme) di protocolli implementati che fornisce un metodo per garantire la sicurezza del protocollo IP, sia esso versione 4 sia 6, e dei protocolli di livello superiore (come ad esempio UDP e TCP), proteggendo i pacchetti che viaggiano tra due sistemi host (es. server), tra due security gateway (ad esempio router o firewall) oppure tra un sistema host e una security gateway</p>
LAN	<p>Local Area Network (LAN) (in italiano rete in area locale, o rete locale), in informatica e telecomunicazioni, indica una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.</p>
Logging	<p>Attività di acquisizione cronologica di informazioni attinenti all'attività effettuata sui sistemi siano essi semplici apparati o servizi informatici</p>
Malware	<p>Malware (abbreviazione dell'inglese malicious software, lett. "software malevole"), in informatica, indica un qualsiasi programma informatico usato per provocare un malfunzionamento più o meno grave dei sistemi e/o rubare di nascosto informazioni di vario tipo. In italiano viene anche comunemente chiamato codice maligno</p>

MAN	In ambito ICT, la Metropolitan Area Network (MAN, in italiano: rete in area metropolitana o più semplicemente rete metropolitana) è un tipo di rete di telecomunicazioni con un'estensione limitata a un perimetro metropolitano. L'interconnessione di più MAN dà vita a reti WAN.
Misure minime di sicurezza	Le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per attuare il livello di sicurezza informatica delle pubbliche amministrazioni, al fine di contrastare le minacce informatiche più frequenti
NAS	Network Attached Storage è un dispositivo collegato alla rete la cui funzione è quella di rendere disponibili grandi spazi di memorizzazione di massa, è costituito da molteplici hardware di memorizzazione di svariate tipologie (es. dischi rigidi, SSD ecc.), all'interno della propria rete
OEM	Original Equipment Manufacturer (produttore di apparecchiature originali). Nella vendita del software applicativo e di sistema trova posto nell'ambito della politica delle licenze d'uso la cessione dei diritti di preinstallazione ai produttori e agli assemblatori di personal computer e sistemi server proprietari. La cosiddetta licenza OEM è rilasciata da importanti produttori di sistemi operativi, di programmi per la grafica, di antivirus. Tale accordo di licenza generalmente prevede la non trasferibilità dei diritti di licenza e altre limitazioni circa la non vendibilità del software separatamente dall'hardware.
Open data	Formato aperto: un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi
Password	Parola Chiave che, congiuntamente allo user-id, consente l'accesso di un utente ad una rete, ad un PC, ad un sistema informatico, o ad un sito Internet
Path	Vedi "Percorso"
Pathname	Concatenazione ordinata del percorso di un file e del suo nome
PEC	La Posta Elettronica Certificata (PEC) è il sistema che consente di inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno, come stabilito dalla normativa
PEO	La Posta Elettronica Ordinaria, vedi definizione di e-mail
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.

Policy	Modello di configurazione e adattamenti da riferirsi a gruppi di utenti o a uso del software
Policy di riferimento	Documento tecnico che descrive lo stato attuale delle policy in uso, aggiornato periodicamente in funzione dell'evoluzione tecnologica/organizzativa
Quietanza di Pagamento	Documento che l'Ente Creditore mette a disposizione del cittadino in seguito alla ricevuta telematica fornitagli da pagoPA.
RDP	RDP (Remote Desktop Protocol) è un protocollo di rete sviluppato da Microsoft, che permette la connessione remota da un computer a un altro in maniera grafica. I client RDP esistono per la maggior parte delle versioni di Microsoft Windows, Linux, Unix, macOS, Android, iOS e altri. I server RDP ufficiali esistono per i sistemi operativi Windows nonostante ne esistano anche per i sistemi Unix-Like. L'applicazione (che usa il protocollo in oggetto) compresa in Windows si chiama Connessione Desktop remoto.
Responsabile per la protezione dati – RPD o DPO	Il Data Protection Officer (di seguito DPO) è una figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 GDPR, pubblicato sulla Gazzetta Ufficiale europea L. 119 il 4 maggio '16. Il DPO è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda/ente (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.
Responsabile per la Transizione al Digitale - RTD	Il Responsabile per la Transizione al Digitale (RTD) ha tra le principali funzioni quella di garantire operativamente la trasformazione digitale della Pubblica Amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di modelli di relazione trasparenti e aperti con i cittadini. L' articolo 17 del Codice dell'Amministrazione Digitale obbliga tutte le amministrazioni a individuare un ufficio per la transizione alla modalità digitale - il cui responsabile è il RTD - a cui competono le attività e i processi organizzativi ad essa collegati e necessari alla realizzazione di un'amministrazione digitale e all'erogazione di servizi fruibili, utili e di qualità.
Rete dati	Insieme dell'infrastruttura passiva (cavi, prese, ecc.) e degli apparati attivi (switch, router, modem ecc.) necessari alla interconnessione di apparati informatici

Router	Un router (letteralmente "intradatore"), in ambito ICT e nell'ambito di una rete informatica a commutazione di pacchetto, è un dispositivo di rete usato come interfacciamento tra sottoreti diverse, eterogenee e non, che lavorando a livello logico come nodo interno di rete deputato alla commutazione, si occupa di instradare i pacchetti dati fra tali sottoreti permettendone l'interoperabilità (internetworking) a livello di indirizzamento
Sandbox	È un processo di rete che consente di inviare i file a un dispositivo separato, da ispezionare senza rischiare la sicurezza della rete. Ciò consente il rilevamento di minacce che potrebbero aggirare altre misure di sicurezza, comprese le minacce zero-day
Server	In informatica e telecomunicazioni è un componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate clients, cioè clienti) che ne fanno richiesta attraverso una rete di computer, all'interno di un sistema informatico o anche direttamente in locale su un computer.
Software	Il software (sigla SW, dall'inglese soft «morbido, leggero» e ware «merci, prodotti», su imitazione del termine hardware), traducibile come componente logico, programma informatico o supporto logico, in informatica ed elettronica è l'insieme delle componenti immateriali (strato logico/intangibile) di un sistema elettronico di elaborazione; è contrapposto all'hardware, cioè la parte materiale (strato fisico/tangibile) dello stesso sistema
Software web-based	Il software che utilizza una interfaccia web per poter essere utilizzato
Spamming	Invio di comunicazioni (prevalentemente di posta elettronica) non sollecitate che contengano materiale pubblicitario; in modo improprio in questa categoria vengono anche catalogate le mail con intenti malevoli (es. truffe, tentativi di furto d'identità, etc.)
SPC	Il Sistema Pubblico di Connettività (SPC) è la rete che collega tra loro tutte le pubbliche amministrazioni italiane, consentendo loro di condividere e scambiare dati e risorse informative. Inoltre è una cornice nazionale di interoperabilità: definisce, cioè, le modalità preferenziali che i sistemi informativi delle pubbliche amministrazioni devono adottare per essere tra loro interoperabili
SPC2	Sistema Pubblico di Connettività e cooperazione fase2
SPCCloud	Sistema Pubblico di Connettività e cooperazione in cloud per l'erogazione di servizi a favore della Pubblica amministrazione
SPID	Sistema Pubblico di Identità Digitale, è la soluzione che permette a tutti i cittadini di accedere ai servizi on-line della Pubblica Amministrazione e dei soggetti privati aderenti con un'unica Identità Digitale utilizzabile da computer, tablet e smartphone

SSID	Acronimo di "service set identifier", cioè il nome che identifica una rete WiFi
SSL	Secure Sockets Layer: protocollo crittografico usato nel campo delle telecomunicazioni e dell'informatica che permette una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti TCP/IP (come ad esempio Internet) fornendo autenticazione, integrità dei dati e confidenzialità operando al di sopra del livello di trasporto.
Storage	<p>In ambito informatico con il termine storage si identificano i dispositivi hardware, i supporti per la memorizzazione, le infrastrutture ed i software dedicati alla memorizzazione non volatile di grandi quantità di informazioni in formato elettronico.</p> <p>Il mercato dello storage è quel settore di mercato ICT che si occupa delle esigenze di memorizzazione di grandi quantità di dati. Esso si può dividere nei seguenti ambiti applicativi:</p> <ul style="list-style-type: none"> • file sharing, ossia tutte le esigenze di condivisione di informazioni tra diversi server e tra i server e i personal computer; • data backup, ossia tutte le esigenze di creazione di copie delle informazioni da riutilizzare nel caso la versione originale venga danneggiata o persa. <p>In italiano un termine che potrebbe sostituire quello inglese è "sistema di archiviazione dati"</p>
Switch	Uno switch (letteralmente "commutatore") è un dispositivo in una rete di computer che collega insieme altri dispositivi. Più cavi di rete sono collegati a uno switch per abilitare la comunicazione tra diversi dispositivi. Gli switch gestiscono il flusso di dati attraverso una rete trasmettendo un pacchetto di rete ricevuto solo a uno o più dispositivi per i quali il pacchetto è destinato. Ogni dispositivo collegato in rete a uno switch può essere identificato dal suo indirizzo MAC, consentendo allo switch di dirigere il flusso del traffico massimizzando la sicurezza e l'efficienza della rete
Traffico	Transito dei dati sulla rete informatica o telefonica
Upload	L'upload, anche noto come "caricamento", in informatica è il processo di invio o trasmissione di un file (o più genericamente di un flusso finito di dati o informazioni) da un client ad un sistema remoto (denominato server) attraverso una rete informatica; l'azione inversa è chiamata download.

UPS	Dalla dicitura in lingua inglese Uninterruptible Power Supply ovvero gruppo di continuità elettrica. E' un'apparecchiatura elettrica utilizzata per ovviare a repentine anomalie nella fornitura di energia elettrica normalmente utilizzata (come cali di tensione e blackout), finanche per erogare costantemente una forma d'onda perfettamente sinusoidale alla frequenza di oscillazione prefissata, priva di variazioni accidentali.
URL filtering	E' il sistema che permette di monitorare e filtrare la navigazione in Internet, bloccando l'accesso a particolari categorie di siti, al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività aziendale
User Id	Identificativo utente, username o nome utente congiuntamente alla password o altri sistemi di sicurezza costituisce le credenziali di accesso ai sistemi
Utente (User)	Persona fisica autorizzata ad accedere ai servizi informatici dell'Ente.
Virtualizzazione	Per virtualizzazione si intende la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente. La virtualizzazione permette l'ottimizzazione delle risorse e la capacità di far fronte a esigenze specifiche secondo il più classico paradigma dell'on demand.
Virus	Per virus informatico si intende un programma o del codice realizzato per danneggiare i computer corrompendone i file di sistema, spreandone le risorse, distruggendone i dati o malfunzionamenti di altro genere. I virus si contraddistinguono da altre forme di malware in quanto sono auto-replicanti, ovvero sono in grado di creare delle copie di se stessi all'interno di altri file o computer senza il consenso o l'intervento di un utente
VOIP	(Voice over IP) tecnologia che rende possibile effettuare una comunicazione telefonica sfruttando il protocollo IP della rete dati
VPN	Virtual Private Network, è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico, condiviso e sicuro attraverso la rete internet
WAN	Una Wide Area Network (WAN) è una rete di telecomunicazioni che si estende su una grande distanza geografica per lo scopo principale della rete di computer. Le reti geografiche sono spesso stabilite con circuiti di telecomunicazione in affitto. Le imprese, l'istruzione e le entità governative utilizzano reti di area vasta per trasmettere dati a personale, studenti, clienti, acquirenti e fornitori da varie località in tutto il mondo. In sostanza, questa modalità di telecomunicazione consente a un'impresa di svolgere efficacemente la propria funzione quotidiana indipendentemente dalla posizione.



COMUNE di SANTO STEFANO DI CAMASTRA

CITTA' METROPOLITANA DI MESSINA
ADERENTE ALL'ENTE PARCO DEI NEBRODI

COMUNE D'EUROPA

AREA funzionale

SVILUPPO TERRITORIALE E GRANDI OPERE – INNOVAZIONE TECNOLOGICA

Servizio 1 – Pianificazione e Gestione Grandi Opere

MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA (MMS)

(Circolare AGID 18/04/2017 n. 2)

ABSC 1: INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	<ul style="list-style-type: none">● Censimento di tutti gli indirizzi IP in uso alla struttura; censimento dell'inventario: ciascun utente della struttura dovrà compilare un form nel quale dovrà indicare i riferimenti tecnici del o dei dispositivo/i che utilizza (es. mac address ovvero modello e numero di serie), e i software (per tipologia o categoria). Etichettare i dispositivi;● Dal punto di vista tecnico tutti i pc, portatili e telefoni VOIP collegati in rete sono gestiti dal DHCP. Quindi accedendo ad uno dei due server attivi è possibile verificare quali sono i dispositivi in esso registrati.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	<p>Nel regolamento comunale è fatto divieto ai dipendenti di utilizzare / collegare alla rete dispositivi non autorizzati.</p> <ul style="list-style-type: none">● Gli inventari di cui al ABSC 1.1.1 vengono aggiornati quando nuove risorse attive vengono collegate in rete.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Vedi ABSC 1.1.1 e 1.3.1

ABSC 2: INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	<ul style="list-style-type: none"> ● Occorre predisporre un documento in cui indicare la lista del software usato nel comune, a partire dai sistemi operativi, al software installato sulle postazioni di lavoro ad uso del personale tecnico amministrativo. Si consiglia di usare un documento condiviso all'interno della struttura in cui abilitare eventuali utenti ad inserire il software utilizzato sulle postazioni di lavoro. 2) Il regolamento ICT vieta l'installazione di software non autorizzato sulle postazioni di lavoro. Su tutte le postazioni sono configurate e sono attive policies di dominio per impedire l'installazione di software da parte dell'utente. L'utente non è amministratore del proprio pc e non ha diritti di accesso a cartelle /porzioni di registro generalmente utilizzate durante l'installazione di software. L'installazione di software sui server è effettuata ESCLUSIVAMENTE da parte dell'Amministratore di sistema previa autorizzazione del RTD. Le postazioni PC sono installate con un'immagine standard che contiene un insieme di software utilizzato in tutto l'ente a cui si aggiungono applicazioni specifiche installate sempre dall'Amministratore di sistema previa autorizzazione del RTD. ● Per i server in gestione a fornitori esterni nella liberatoria per l'accesso remoto viene indicato il software presente ed è riportata una clausola per cui l'ente dovrà autorizzare preventivamente qualsiasi software sia necessario aggiungere. Questa clausola verrà indicata anche nella nomina ad amministratori esterni nell'ambito delle attività per l'adeguamento al GDPR.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	<ul style="list-style-type: none"> ● L'amministratore di sistema (o il RTD) effettua verifiche periodiche, documentando il risultato.

ABSC 3: PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, PC E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	<ul style="list-style-type: none"> ● Tutte le postazioni pc vengono create e gestite con un'immagine standard e con policies di dominio. L'immagine standard è stata creata con l'obiettivo di limitare le azioni degli utenti che possano compromettere la propria postazione o la rete dell'ente. L'utente, pertanto, non può installare software, modificare configurazioni (es. impostazioni dei browser installati, associazione delle estensioni), creare/modificare utenti e gruppi locali, modificare i permessi su file system ecc.

ABSC 3: PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, PC E SERVER						
ABSC_ID			Livello	Descrizione	Modalità di implementazione	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Vedi 3.1.1	
	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	<ul style="list-style-type: none"> In caso di compromissione di una postazione PC si provvede alla formattazione e alla ricreazione ex novo con le modalità suddette e alla reinstallazione dei software specifici. Eventuali dati salvati in locale (e non in rete come suggerito dalle direttive dell'ente) sulla postazione, saranno successivamente ripristinati da un back-up, se disponibile. In caso di compromissione di un server, è fondamentale capire quando è avvenuta la compromissione e qual è il livello di gravità/invasività. 	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	<ul style="list-style-type: none"> Le immagini dei pc non sono memorizzate offline ma vengono costruite con un processo che le rende altrettanto sicure. L'immagine finale è infatti costruita in modo dinamico partendo dall'ISO del sistema operativo ed applicando una Task sequence. All'immagine standard si aggiungono dinamicamente policies di dominio modificabili solo dagli amministratori del dominio stesso. 	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	<ul style="list-style-type: none"> Tutte operazioni di amministrazione remota vengono fatte utilizzando protocolli sicuri: ad esempio SSH per i server Linux ed apparati di rete, Https per storage/appliance/ambiente virtuale, RDP per i server Windows. Qualora sia necessario utilizzare un protocollo non criptato l'accesso è consentito solo ai pc nei locali del servizio gestione e sviluppo delle tecnologie. 	

ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ						
ABSC_ID			Livello	Descrizione	Modalità di implementazione	
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	<ul style="list-style-type: none"> E' installata su tutti i pc l'antivirus freeware Avast Per le infrastrutture di rete il monitoraggio avverrà, dopo la nomina di un Amministratore di Sistema, tramite piattaforma dedicata. È competenza dell'amministratore di sistema effettuare, con cadenza mensile, la procedura di monitoraggio e di vulnerability assessment, nonché l'aggiornamento degli antivirus ogni volta venga rilasciato un aggiornamento del codice o della base dati. 	

ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	<ul style="list-style-type: none"> • Vedi ABSC 4.1.1 • Il servizio utilizzato per le scansioni di vulnerabilità è effettuato tramite una sonda installata in rete e gestito da una ditta specializzata in sicurezza ICT. L'aggiornamento dello strumento è pertanto garantito essendo fondamentale per assicurare l'efficienza del loro servizio
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	<ul style="list-style-type: none"> • Gli aggiornamenti sono automatizzati limitatamente alle postazioni di lavoro. In ambito server (appliance) vengono installate automaticamente solo patch critiche e di sicurezza (security updates)
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	<ul style="list-style-type: none"> • Vedi ABSC 4.1.1 • All'interno del comune non esistono sistemi air-gapped
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	<ul style="list-style-type: none"> • Vedi ABSC 4.1.1. Inoltre, è competenza dell'amministratore di sistema verificare che le vulnerabilità emerse dalle scansioni dei software siano effettivamente sanate dopo l'installazione di patch o di azioni correttive che ne limitano il possibile rischio
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	<ul style="list-style-type: none"> • Vedi ABSC 4.1.1
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In	Vedi ABSC 4.8.1 e 4.1.1

ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ				
ABSC_ID		Livello	Descrizione	Modalità di implementazione
			particolare, applicare le patch per le vulnerabilità a partire da quelle più critiche.	

ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE				
ABSC_ID		Livello	Descrizione	Modalità di implementazione
5	1	1	M Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	<p>L'accesso ai sistemi con privilegi amministrativi è consentito solo all'Amministratore di sistema e al Responsabile per la Transizione Digitale (o un suo delegato che abbia le competenze ed effettive necessità di modificare la configurazione dei sistemi). Come regola generale si cerca di evitare di dare i privilegi amministrativi, ma eventualmente di dare l'accesso con ruolo "user" o di abilitare solo le funzioni necessarie (es: accesso a cartelle specifiche, possibilità di eseguire alcuni task, possibilità di riavviare alcuni servizi).</p> <p>Gli utenti non hanno privilegi amministrativi sui pc.</p> <p>Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata al RTD che autorizza l'installazione da parte dell'Amministratore di Sistema, affinché provveda all'installazione e ad aggiornare l'elenco.</p> <p>Le abilitazioni all'installazione del software sono concesse solamente all'amministratore di sistema.</p> <p>Per i server in gestione alle ditte esterne qualora la ditta debba avere accessi amministrativi questi saranno limitati solo al server in gestione.</p>
5	1	2	M Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	<ul style="list-style-type: none"> Sui server gli accessi vengono registrati attraverso apposito software di log. Sui PC Clients il solo utente amministratore (esclusi gli amministratori di rete) è l'utente locale chiamato "amministratore", il quale viene gestito dall'Amministratore di Sistema su tutti i PC e con uguale password.

ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	<ul style="list-style-type: none"> Le utenze amministrative sono rilasciate nominalmente. Da Active Directory si possono ricavare tutte le utenze amministrative rilasciate. L'Amministratore di sistema è nominato formalmente con un atto da parte del Sindaco (d'intesa con il RTD) oppure direttamente dal Responsabile per la Transizione al Digitale.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	<ul style="list-style-type: none"> Prima di collegare alla rete un dispositivo le password di default degli utenti amministratori vengono sostituite con altre corrispondenti alle regole dell'ente.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	<ul style="list-style-type: none"> Questa misura è rispettata dall'adozione della password policy contenuto nel Regolamento per la sicurezza delle informazioni
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	<ul style="list-style-type: none"> Il Regolamento per la sicurezza delle informazioni prevede che le utenze amministrative vengono sostituite ogni tre mesi.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	<ul style="list-style-type: none"> Il Regolamento per la sicurezza delle informazioni prevede che le vecchie password non possono essere riutilizzate prima di sei modifiche
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Vedi 5.1.2
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze sono nominative e riconducibili alla singola persona
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	È stata data istruzione agli amministratori di sistema di utilizzare le credenziali amministrative anonime solo in caso di emergenza o per eseguire servizi o attività pianificate che debbano avere questo tipo di privilegi per funzionare. In quest'ultimo caso è in corso di verifica la possibilità di configurarle in modo da poter essere usate solo per quello scopo e non per attività interattive o per connettersi ai server.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	<ul style="list-style-type: none"> Da Active Directory si possono ricavare tutte le utenti amministrative rilasciate

ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	<ul style="list-style-type: none"> Non sono disponibili certificati digitali.

ABSC 8: DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	<p>Su tutte le PDL a dominio attualmente è attivo il prodotto fornito da Windows 10 denominato Windows Defender.</p> <p>Per le postazioni con sistema operativo antecedente al Windows 10, nell'attesa di procedere all'aggiornamento del sistema operativo, è installato l'antivirus freeware Avast. Gli utenti non amministratori sono inibiti a disattivare l'antivirus e gli aggiornamenti.</p>
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	<ul style="list-style-type: none"> Su tutti i dispositivi è attivo il firewall, filtro email, filtro spam e filtro web garantito dall'acquisto del servizio denominato "Endian UTM Mercury HW50 Maintenance 3y"
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	<ul style="list-style-type: none"> Il regolamento per la sicurezza delle informazioni vieta l'uso ed il collegamento in rete di dispositivi non autorizzati.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimovibili.	<ul style="list-style-type: none"> Attivare una Group Policy Object sul dominio che disattiva su tutti i PC l'esecuzione automatica dei contenuti sui dispositivi rimovibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	<ul style="list-style-type: none"> Su Microsoft Office, dalla versione 2007, è prevista l'opzione di configurazione che prevede un messaggio di accettazione prima di eseguire qualsiasi macro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	<ul style="list-style-type: none"> Impostare la sola visualizzazione delle intestazioni.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	<ul style="list-style-type: none"> Impostare la configurazione standard dei PDL con l'opzione Disattiva l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	<ul style="list-style-type: none"> Impostare come regola nel software antivirus. "Avast" installato nei PC

ABSC 8: DIFESE CONTRO I MALWARE						
ABSC_ID			Livello	Descrizione	Modalità di implementazione	
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antisпам.	In tutte le caselle di posta sono attivati filtri anti malware e anti spam attraverso il servizio "Endian UTM Mercury HW50 Maintenance 3y-R"	
8	9	2	M	Filtrare il contenuto del traffico web.	<ul style="list-style-type: none"> ● Attivare il filtro del contenuto del traffico web per mezzo del firewall perimetrale comunale. Vengono bloccate le seguenti categorie: <ul style="list-style-type: none"> ○ P2P, ○ Lottery, ○ Sexual Subject ○ Streaming media, ○ Forum, ○ Vulgar/gruesome, ○ Gambling, ○ Drugs, ○ Malicious WebSites, ○ Pornography Web Sites ○ Tutto il traffico verso Cina, Russia, Corea Nord <p>Il filtro al traffico web viene applicato attraverso il servizio "Endian UTM Mercury HW50 Maintenance 3y-R"</p>	
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	<ul style="list-style-type: none"> ● attivare policies sulle appliance Antispam per rimuovere allegati potenzialmente pericolosi. Sul firewall sono attive regole per evitare il download di file con estensioni (es: exe, zip, jar, ecc.) che possono avere contenuti malevoli. Tutte le azioni anzidette sono garantite dal servizio "Endian UTM Mercury HW50 Maintenance 3y-R" 	

ABSC 10: COPIE DI SICUREZZA						
ABSC_ID			Livello	Descrizione	Modalità di implementazione	
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	<ul style="list-style-type: none"> ● Le copie di sicurezza di tutti i sistemi server/database/posta verranno fatte giornalmente provvedendo all'acquisto di un software di Cloud Backup on line certificato). ● Il backup dei dati e gli applicativi in Cloud sono garantiti dai contratti con i fornitori. 	

ABSC 10: COPIE DI SICUREZZA					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	<ul style="list-style-type: none"> I dispositivi su cui vengono effettuate tutte le copie di sicurezza devono essere custoditi in locali con accesso controllato e consentito solo all'Amministratore di sistema o il RTD. Tali locali devono essere protetti da sistemi di videosorveglianza e antifurto.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	<ul style="list-style-type: none"> I dispositivi su cui vengono fatte le copie presso l'ente non devono essere direttamente accessibili come unità di rete.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI					
ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	<p>Predisposizione di un'analisi dei livelli particolari di riservatezza con conseguente compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL). Ad esempio, i dati sui residenti che chiedono assistenza ai Servizi Sociali, l'elenco dei tributi, le sanzioni emesse dalle Polizia Locale, ecc.).</p> <p>Nell'ambito del processo di adeguamento alla normativa sulla protezione dei dati, viene condotta un'analisi dei dati, finalizzata all'individuazione dei dati che, per la loro natura, necessitano di ulteriori misure di sicurezza. In quest'ultimo caso, si procederà all'attivazione, di concerto con l'Amministratore di sistema (o il gestore del servizio Cloud), della protezione crittografica.</p>
13	8	1	M	Bloccare il traffico da e verso URL presenti in una blacklist.	Vedi ABSC 8.9.2



DI MAURO IL RESPONSABILE TRANSIZIONE DIGITALE
 Danilo (Dott. Ing. Danilo Di Mauro)
 14.03.2025
 12:35:31
 GMT+01:00

Il presente verbale, dopo la lettura, si sottoscrive per conferma.

IL PRESIDENTE
F.to: Re

L'ASSESSORE ANZIANO
F.to: Amoroso

IL SEGRETARIO GENERALE
F.to Testagrossa

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto Segretario Generale certifica che la presente deliberazione è copia conforme all'originale ed è pubblicata all'Albo Pretorio il 24.03.2025

Li, 24.03.2025



IL SEGRETARIO GENERALE
Dott. ssa Anna A. Testagrossa

CERTIFICATO DI ESECUTIVITA'

- è stata resa immediatamente esecutiva, ai sensi dell'art. 16 della L.R. 3/12/1991 n.44;
- è divenuta esecutiva il _____ decorsi dieci giorni dalla relativa pubblicazione all'Albo Pretorio, ai sensi dell'art. 12 della L.R. 03/12/1991 , n. 44.

Li, 24.03.2025



IL SEGRETARIO GENERALE
Dott. ssa Anna A. Testagrossa

CERTIFICATO DI AVVENUTA PUBBLICAZIONE

Si certifica che la presente deliberazione:

- è stata pubblicata all'Albo pretorio per 15 giorni consecutivi dal _____ al _____ come previsto dall'art.11 L.R n.44/91, giusta attestazione del messo comunale.

Li,

IL SEGRETARIO GENERALE
Dott. ssa Anna A. Testagrossa