Regolamento comunale

PER L'UTILIZZO DEI SISTEMI INFORMATICI

Attività	*Atto*	*Organo*	*N.ro*	*Data*	*Esecutività*
Approvazione	Delibera	Giunta Comunale	000	00.00.0000	00.00.0000

SOMMARIO

Premessa

Il presente documento intende fornire le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.
Ogni utente, intendendosi con ciò ogni dipendente, senza distinzione di ruolo e/o di livello e ogni collaboratore ed organo politico in possesso di specifiche credenziali di autenticazione per l'accesso alle risorse informatiche dell'Ente, è tenuto a rispettare il presente regolamento, che è reso disponibile tramite le modalità specificate al punto 23.
Si specifica che tutti gli strumenti utilizzati dagli utenti per prestare la propria attività lavorativa, intendendo con ciò, ad esempio, PC, notebook, strumenti informatici, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "strumenti"), sono messi a disposizione dall'Ente, come dispositivi o come servizio (DaaS – Desktop as a service e SaaS – Software as a service); ma è anche consentito l'utilizzo di dispositivi propri (BYOD[1]) per rendere la prestazione lavorativa al di fuori della rete comunale.
In ogni caso, sui dispositivi di proprietà degli utenti, sia utilizzati come terminali del desktop remoto, sia per accedere a risorse disponibili sul web, non sono previste né l'installazione di programmi e/o procedure comunali né l'impiego di alcun sistema di monitoraggio delle attività e/o delle connessioni.
Le disposizioni contenute nel presente regolamento si applicano, a compendio delle regole definite dall'Ufficio competente, anche ai dispositivi mobili (smartphone e tablet) in grado di interconnettersi all'infrastruttura di rete ed ai relativi servizi.
I dati personali e le altre informazioni degli utenti, registrati automaticamente negli strumenti durante il loro uso (log di sistema), sono memorizzati sui dispositivi stessi e possono essere utilizzati per la sicurezza della postazione e per la tutela del patrimonio;
Per "tutela del patrimonio" si intende altresì la sicurezza informatica e la tutela del sistema informatico.
Tali informazioni sono raggiungibili solo dall'amministratore di sistema, nei casi previsti dalla Legge, con gli strumenti nativi dei sistemi operativi.
Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori. Sono però monitorati i log di sistema e le connessioni.

[1] *Il termine BYOD (Bring Your Own Device) indica la pratica organizzativa che consente ai dipendenti di utilizzare i propri dispositivi personali — laptop, smartphone o tablet — per accedere a risorse e servizi aziendali. La policy BYOD richiede adeguate misure di sicurezza per garantire la protezione dei dati e la conformità alle procedure interne.*

1 - Oggetto e finalità

1.1 - Il presente regolamento è redatto sulla base della seguente normativa:

- Legge 20. 05.1970, n. 300, recante *"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";*
- *"Linee guida del Garante per posta elettronica e internet"* in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- Regolamento Europeo 679/16 *"General Data Protection Regulation*" (d'ora in avanti Reg. 679/16 o GDPR);
- Codice penale, con particolare riferimento ai reati informatici;
- D. Lgs. 82/2005 e s.m.i. *"Codice dell'amministrazione digitale";*
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le *"Linee guida per posta elettronica e Internet"* di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i *"Testo Unico sulla sicurezza";*
- D.P.R 62/2013 *"Codice di comportamento dei dipendenti della pubblica amministrazione";*

1. 2 - La finalità del presente documento è quella di promuovere in tutti gli utenti una corretta *"cultura informatica"*, definire le norme di comportamento per l'uso degli strumenti messi a disposizione dall'Amministrazione, fornire le indicazioni necessarie per evitare il verificarsi di qualsiasi uso non conforme o abuso dei succitati strumenti ed informare gli utenti rispetto alle attività memorizzate nei log di sistema.

2 - Principi generali e principi di riservatezza nelle comunicazioni

2.1- I principi che sono a fondamento del presente regolamento sono gli stessi espressi nel GDPR, e, precisamente:

a) il principio di liceità, secondo il quale ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del GDPR: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.
b) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);
c) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori;
d) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 5, commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2.2 -L'utente si attiene alle seguenti regole di trattamento dati:

a) è vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari e giudiziari, elementi e informazioni dei quali l'utente viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al Responsabile del servizio in cui opera;
b) è vietata l'estrazione per uso personale di originali e/o copie cartacee ed informatiche di documenti, fascicoli, lettere, data base e quant'altro determinato dall'Ente o per ragioni d'ufficio.

2.3 - Le misure per il trattamento dei dati personali e le procedure da adottarsi in caso di data breach sono contenuti in appositi provvedimenti adottati dall'Ente (a riguardo vedasi DGC n. 83 del 17.08.2021 ad oggetto "APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)"relativamente alla procedura di

gestione dei cd. *data breach* e DGC n. 113 del 06.12.2023 ad oggetto " PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO A TUTELA DEI DATI PERSONALI. APPROVAZIONE." relativamente alle modalità di trattamento dati ed al modello organizzativo dell'Ente).
2. 4 -L'Ente effettuerà tramite l'Amministratore di Sistema, inoltre, attività di monitoraggio e verifica dell'efficacia delle misure di protezione predisposte sul sistema informativo rispetto ad aggressioni esterne senza che siano necessarie preventive ulteriori informative. Le risultanze di tali attività di monitoraggio e verifica potranno essere utilizzate soltanto in modo proporzionato e pertinente alle finalità e alla natura delle stesse e non, ad esempio, al fine di attuare indirettamente un controllo a distanza dell'attività lavorativa svolta dall'utente.

3 - Tutela del lavoratore

3.1- Alla luce dell'art. 4, comma 1, L. n. 300/1970, le disposizioni di cui al presente regolamento non sono finalizzate all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze di servizio e di sicurezza nel trattamento dei dati personali.
3.2 - È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del GDPR 679/16.

4 - Titolarità e descrizione dell'architettura dei servizi informatici

4.1- Ogni postazione di lavoro all'interno degli uffici comunali è dotata di una connessione di rete di dominio sulla quale transitano sia i servizi informatici che quelli di telefonia fissa (VoIP).
4.2 - In aggiunta alla connessione di rete tramite cavo, può essere disponibile il servizio di rete Wi-Fi; attraverso la tecnologia Wi-Fi è possibile connettersi sia alla rete aziendale, che prevede l'autenticazione automatica dei dispositivi dell'Ente iscritti al dominio, sia alla rete pubblica.
4.3 - Attraverso qualsiasi dispositivo idoneo collegato alla rete di dominio ogni utente può connettersi al proprio desktop remoto personale (RDP), il cui accesso non è abilitato in modo automatico. Gli utenti dotati di postazione di lavoro fissa possono accedere al proprio desktop tramite VPN solo previa autorizzazione del CED e relativa abilitazione tecnica. In assenza di tale autorizzazione, l'accesso remoto avviene esclusivamente tramite piattaforma TSplus, attraverso la quale l'utente può utilizzare applicativi e accedere alle proprie cartelle di rete, senza disporre di un desktop remoto personale. Gli utenti dotati di laptop assegnato dall'Ente dispongono già del proprio ambiente desktop anche al di fuori della rete comunale e possono accedere alle cartelle di rete avviando la VPN preinstallata sul dispositivo.
4.4 - L'Amministrazione comunale, nella scelta dei programmi per elaboratore elettronico, privilegia quelli appartenenti alla categoria del software libero ed i programmi il cui codice è ispezionabile dal titolare della licenza. Qualora si renda necessaria l'acquisizione di programmi software, si adottano le prescrizioni di cui al Codice dell'Amministrazione Digitale (CAD) e alle relative Linee guida definite dall'Agenzia per l'Italia Digitale (AgID).
4.5 - Il Comune di Borghetto Santo Spirito è titolare di tutte le risorse informatiche. Il personale dipendente e/o assimilato deve essere informato sugli usi consentiti e vietati di tali risorse. Ogni violazione delle regole per un uso corretto del Sistema Informatico Comunale costituisce una violazione della sicurezza e potrà comportare l'applicazione dei provvedimenti disciplinari previsti.

5 - Amministrazione di Sistema

5.1 - L'Ente conferisce all'Amministratore di Sistema il compito di sovrintendere i beni e le risorse informatiche aziendali. È compito dell'amministratore di sistema:
1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Ente;

2) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati
5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
6) provvedere alla sicurezza informatica dei sistemi informativi aziendali, nel rispetto di quanto prescritto dal D. Lgs. 196/2003 (artt. 31 e 33) e ss. mm. Ii;
7) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di Responsabile Privacy all'interno dell'Ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto;
8) Quant'altro previsto dall'appalto per la gestione del servizio informatico;

5.2 - L'Amministratore delle risorse tecnologiche condivise e delle applicazioni svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite dall'Ente e nel rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali.
5.3 - Qualora si renda necessario procedere ad operazioni finalizzate al ripristino della funzionalità del Sistema informativo comportanti l'accesso a cartelle, file o archivi di altri utenti, l'Amministratore di rete è tenuto ad avvisare preventivamente gli interessati, limitando il proprio intervento a quanto strettamente necessario.

6 - Gestione, assegnazione e revoca delle credenziali di accesso al dominio, alla posta elettronica e alle procedure con autenticazione propria.

6.1 - Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate secondo il processo di de/provisioning e moving del personale.
6.2 - Le credenziali di autenticazione relative ai diversi ambiti, consistono in:

a) una username per l'accesso al dominio comunale e relativa password;
   - ➔ per i dipendenti dell'Ente la username coincide con *nome.cognome*;
   - ➔ per le altre persone abilitate ad accedere al dominio (collaboratori/organi politici) la username è personalizzata in funzione della tipologia contrattuale in essere con l'Amministrazione
b) una login per l'accesso al sistema di posta elettronica e servizi di rete associati, del tipo *nome.cognome@comune.borghettosantospirito. sv.it;* è garantita la gestione di credenziali univoche in caso di omonimia;

6.3 - Per ogni evento riguardante ciascun utente (assunzione, cessazione, mobilità) l'ufficio competente provvede alla tempestiva informazione della variazione all'Amministratore di Sistema deputato alla gestione delle credenziali medesime.
6.4 - Abilitazioni, disabilitazioni e profilazione nell'accesso alle procedure e/o alle cartelle di rete avvengono, su istanza del Responsabile del servizio e ad opera dell'Amministratore di sistema, in coerenza alle modalità di svolgimento delle funzioni e delle singole attività all'interno dell'Ente e nel rispetto della normativa in materia di privacy. È necessario che ogni Responsabile del servizio consideri come le singole attività sono attribuite e svolte dai dipendenti loro assegnati con particolare attenzione alla configurazione del trattamento dei dati personali che ne deriva e alle relative autorizzazioni e profilazioni specifiche per utente e per applicativo utilizzato.

6.5 - Le credenziali di accesso alle risorse informatiche devono essere periodicamente modificate (ogni 90 giorni) e rispettare regole di sicurezza nella loro composizione. Il periodo di validità e le regole applicate possono variare a seconda degli applicativi interessati (di norma la password deve rispettare contemporaneamente i seguenti requisiti minimi di complessità:

- almeno 14 caratteri;
- uso di lettere maiuscole e minuscole;
- numeri e caratteri speciali oltre, preferibilmente a non contenere parole di senso compiuto;

6.6 - In caso l'utente dimentichi (o faccia scadere) la password di accesso ad un servizio, se non è disponibile una procedura autonoma, presenterà richiesta di reset – tramite apposito ticket - della stessa all'ufficio CED competente che verificherà l'identità del richiedente prima del rilascio della nuova password.

7 - Strumenti informatici (PC – fisico o desktop remoto, notebook e altri strumenti con relativi software e applicativi) di proprietà dell'Ente.

7. 1 - L'utente è consapevole che gli strumenti di proprietà dell'Ente sono forniti per rendere la prestazione lavorativa e per scopi professionali, estendendo a tale ambito anche quelli connessi alla ricerca, alla didattica e alla crescita delle competenze nell'uso delle tecnologie dell'informazione e della comunicazione. Ognuno è responsabile dell'utilizzo degli strumenti assegnati dall'Amministrazione ed ha il compito di farne un uso conforme ai principi di diligenza sanciti dal codice civile; ciascun utente si deve quindi attenere alle regole di utilizzo degli strumenti di cui al presente regolamento oltre a quanto vietato dal c.p.
7.2 - L'accesso agli strumenti è protetto da password; per il primo accesso devono essere utilizzate le credenziali fornite dall'Amministratore di sistema (cfr. punto 6. 2), la password deve essere quindi modificata dall'utente con una personale. A tal proposito si rammenta che le credenziali sono strettamente private e l'utente è tenuto a conservarle nella massima segretezza.
7.3 - Le postazioni informatiche (monitor, pc e gruppo di continuità etc…) assegnato viene identificato univocamente da uno o più numeri di inventario Comunale, deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione delle password d'accensione (BIOS[2]) e protezione disco, senza preventiva autorizzazione da parte dell'Amministratore di sistema.
Ogni dispositivo hardware, indipendentemente dall'assegnazione, può essere utilizzato da tutti gli utenti in possesso delle credenziali di accesso al dominio; nel caso di dispositivi con sistema operativo Windows viene creata un'area riservata sul disco locale per ogni utente che ha avuto accesso allo stesso. Al fine di garantire la riservatezza e sicurezza dei propri dati è necessario memorizzarli sulle share (cartelle) di rete (cfr. punto 8 – infrastruttura di rete).
7.4 - Le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati secondo standard decisi dall'Amministrazione comunale e volti a garantire la fruizione di tutti i servizi necessari allo svolgimento delle mansioni degli utenti. Lo stesso non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione da parte del Servizio competente, su richiesta dell'Amministratore di sistema attraverso la procedura definita, in funzione di particolari attività che necessitano di software o impostazioni ad hoc.
7.5 - L'installazione sui personal computer di sistemi operativi e programmi applicativi e, in generale, di software, avviene ad opera dei tecnici informatici incaricati, che operano seguendo i necessari criteri di sicurezza. L'uso di tali programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta indicate.

[2] *Il BIOS (Basic Input/Output System) è il firmware che inizializza l'hardware del computer all'avvio e controlla il processo di boot. L'impostazione di una password BIOS blocca l'accesso al sistema prima ancora del caricamento del sistema operativo, garantendo una protezione di base contro accessi non autorizzati.*

7. 6 - L'installazione di programmi da parte dell'utente, ove sia consentito dal personal computer e dalle relative impostazioni, deve avvenire senza aggirare divieti o restrizioni eventualmente previsti, nel pieno rispetto delle condizioni che disciplinano l'utilizzo di tali programmi e, in generale, della normativa vigente, con particolare riferimento alle disposizioni in materia di protezione di diritti di proprietà intellettuale: abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro. In ogni caso, l'utente sarà responsabile e sarà chiamato a manlevare e tenere indenne l'Amministrazione comunale da qualsiasi danno o richiesta di risarcimento che venga avanzata da soggetti terzi.
7.7 - Tutti i software presenti sui personal computer al momento della consegna ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi.
7.8 - L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare uno strumento incustodito con una sessione di lavoro attiva può essere causa del suo utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso, è presente un automatismo di "blocco" che si attiva trascorsi 15 minuti di inattività.
7.9 - È obbligatorio consentire l'installazione degli aggiornamenti di sistema operativo che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.
Per gli aggiornamenti degli applicativi proposti durante il loro uso è necessario l'intervento dell'Amministratore di Sistema che provvederà a rilasciarli dopo averne verificato la compatibilità con le policy di sicurezza e con i sistemi informativi coinvolti.
7.10 - È vietato utilizzare i dispositivi informatici per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright, così come non è ugualmente ammesso connettere alla rete locale cablata o alla rete di dominio qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di sistema.
7.11 - Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema tramite apposito Help Desk (cfr. punto 9).
7.12 - In regime di telelavoro e lavoro agile si applicano anche le ulteriori disposizioni previste dai relativi disciplinari e dai contratti individuali.
7.13 - In caso di furto e/o smarrimento è compito dell'utente assegnatario dell'attrezzatura presentare denuncia all'autorità giudiziaria ed informare, inoltrando copia della denuncia presentata al Responsabile del servizio di appartenenza, all'Amministratore di sistema e i Servizi coinvolti nella gestione delle attrezzature per gli ulteriori adempimenti.

8 - Infrastruttura di rete, servizi Cloud e File System

8.1 - Il dominio dell'Ente, "BORGHETTO.LOCAL", comprende tutti i servizi di identificazione utente e accesso personalizzato alla rete aziendale, al suo file system e alle altre risorse di rete e di stampa condivise.
8.2 - Per l'accesso al dominio dell'Ente, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto previsto al punto 6.2.
8.3 - È vietato accedere alla rete ed ai sistemi informativi utilizzando credenziali di altri utenti.
8.4 - L'accesso al dominio garantisce all'utente:

- la disponibilità dei dispositivi multifunzione di stampa e delle share di rete (cartelle condivise su server);
- cartella condivisa della struttura di assegnazione;
- cartella comune denominata *"Area di Condivisione"* utilizzabile da tutti gli utenti del dominio, destinata allo scambio di documenti e file, nel rispetto della normativa privacy, tra utenti di strutture diverse;
- eventuali altre cartelle condivise, rese disponibili secondo specifica abilitazione (cfr. 6.4).

Tutte le cartelle di rete, siano esse condivise o personali, ospitano esclusivamente contenuti professionali e sono quotidianamente oggetto di backup. Inoltre, queste sono attualmente in ambiente cloud qualificato come individuato dall'Ente.
8.5 - Tutte le risorse di memorizzazione diverse da quelle citate al precedente punto 8.4 non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o in disponibilità personale come hard disk portatili. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché la sicurezza e la protezione contro la loro eventuale perdita non sono garantite; pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.
8.6 - I dati trattati dall'Ufficio devono essere custoditi esclusivamente sugli elaboratori server e gestiti mediante gli elaboratori client del Sistema Informatico dell'Ente, in quanto appositamente predisposti per garantire le necessarie doti di sicurezza, integrità e protezione. È espressamente vietata la custodia e la gestione di dati di proprietà del Comune di Borghetto Santo Spirito su supporti rimovibili di qualsiasi tipo. Qualora l'utilizzo di supporti rimovibili sia necessario per attività non ordinarie, essi devono essere riposti, dopo l'utilizzo, in appositi armadi chiusi a chiave, onde evitare divulgazione, alterazione, furto o recupero non autorizzato dei dati. La distruzione o inutilizzabilità dei supporti rimovibili deve avvenire seguendo le istruzioni del personale del competente ufficio CED.
8.7 - Nell'ipotesi di assenza o impossibilità temporanea o protratta dell'utente, qualora per ragioni di sicurezza o per garantire l'ordinaria operatività dei servizi sia necessario accedere a documenti di lavoro presenti sui dispositivi o sulla share personale, l'utente può delegare, in accordo con il proprio Responsabile, un fiduciario della sua stessa struttura per individuare e inoltrare i documenti rilevanti. La delega si esprime come richiesta all'Amministratore di Sistema di temporanea abilitazione. Delle attività svolte devono essere informati l'utente interessato e l'Amministratore di Sistema.
8.8 - Qualora l'utente non abbia delegato un fiduciario, in caso di straordinaria necessità il Responsabile del servizio può richiedere, con apposita motivazione, all'Amministratore di Sistema di accedere alla share o ai dispositivi dell'utente assente; di tale attività deve essere redatto verbale e informato l'utente interessato.
8.9 - È vietato l'utilizzo di piattaforme cloud non autorizzate dall'Ente per la condivisione di file con soggetti esterni, al fine di garantire la tutela dei dati personali e la certezza della loro conservazione. L'unico sistema ammesso per la condivisione esterna è il servizio di webmail dell'Ente**,** che assicura l'archiviazione dei documenti sui medesimi server utilizzati per la posta elettronica e sotto la responsabilità del relativo fornitore del servizio.
Gli utenti devono adottare tutte le misure di sicurezza previste dal Regolamento (UE) 679/2016, garantendo integrità e riservatezza dei file trattati.
8.10 - Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia delle cartelle su server, con cancellazione dei file obsoleti o inutili, evitando duplicazioni e archiviazioni ridondanti.
8.11 - L'Amministratore di Sistema può negare o interrompere l'accesso alla rete ai dispositivi non adeguatamente protetti e/o aggiornati, che costituiscono minacce per la sicurezza informatica.
8.12 - Per gli utenti in telelavoro o lavoro agile si applicano le disposizioni dei relativi disciplinari.
8.13 - Lo smaltimento dei supporti informatici e dei dispositivi elettronici deve avvenire secondo le disposizioni del Provvedimento del Garante del 13 ottobre 2008 (G.U. n.297 del 9 dicembre 2008) e nel rispetto delle procedure per RAEE, garantendo la protezione dei dati personali.

9 - Help Desk

(I dettagli relativi al funzionamento del servizio di Help Desk sono disponibili alla relativa pagina pubblicata sulla Intranet comunale (link operativo solo per consultazione all'interno della rete comunale)

9.1 - Il servizio di Help Desk è raggiungibile mediante il numero telefonico interno (con deviazione al fornitore del servizio) appositamente assegnato e mediante l'indirizzo mail ced@comune.borghettosantospirito.sv.it (oltre ad altri eventuali specifici indirizzi mail indicati dal fornitore).

9.2 - A fronte della segnalazione telefonica il servizio di Help Desk cerca di formulare una diagnosi del malfunzionamento intervenendo direttamente per quanto possibile.
9.3. - Per ogni segnalazione registrata, il servizio di Help Desk è tenuto ad aprire un'apposita procedura di assistenza sull'apposito applicativo in essere e darne visibilità all'utente. Lo stesso ticket verrà chiuso a fronte della risoluzione del problema e anche della chiusura deve essere informato l'utente originatore della segnalazione. Le tempistiche sono determinate in sede di appalto.

10 - Regole applicabili all'utilizzo di internet mediante gli strumenti informatici dell'Ente

(Le regole specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007 e s. m. i..)
10.1 - La rete internet può e deve essere utilizzata dall'utente a supporto dell'attività lavorativa.
10.2 - È favorito l'uso, di norma attraverso l'interfaccia web, di strumenti di messaggistica istantanea e servizi di videoconferenza e collaborazione on line, per permettere una efficace e comoda comunicazione sia tra i colleghi, sia con interlocutori esterni all'Ente. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche e alle e-mail.

11 - Utilizzo della posta elettronica istituzionale

11.1 - Ad ogni utente viene fornito un account e-mail nominativo.
11.2 - L'insieme degli indirizzi di posta nominativi costituisce la rubrica globale del Comune di Borghetto Santo Spirito ed è disponibile nella piattaforma di gestione della posta. Trattandosi di dati personali possono essere divulgati esclusivamente per fini istituzionali.
11.3 - L'Ente fornisce, altresì, delle caselle di posta elettronica condivise associate a unità organizzative, uffici o gruppi di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative per le comunicazioni di tipo procedimentale. È compito dell'Amministratore di Sistema provvedere, su richiesta dei Responsabili di Servizio, alla creazione e/o la eliminazione delle caselle di posta condivise e gestire le abilitazioni e/o disabilitazioni degli utenti alle stesse, definendone il relativo livello di delega.
11.4 - L'utilizzo dell'e-mail deve essere finalizzato allo svolgimento delle proprie mansioni lavorative e alle comunicazioni relative alle stesse, conformemente al punto 7. 1. Si ricorda che gli indirizzi delle caselle di posta elettronica forniti dall'Ente di norma non devono essere utilizzati, in particolare in modo massivo, per fini non connessi all'attività lavorativa. (ad esempio l'invito a partecipare ad eventi extra lavorativi).
11.5 - È compito di ogni utente provvedere alla costante eliminazione delle mail non necessarie al fine di contenere le dimensioni degli archivi di posta. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle cartelle di rete.
11.6 - L'iscrizione a mailing-list o newsletter esterne con l'indirizzo fornito dall'Amministrazione è ammessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
11.7 - Allo scopo di garantire sicurezza alla rete, l'utente deve evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito oppure che contengono allegati con contenuto di tipo attivo come, ad esempio, *. exe, *. com, *. vbs, *. htm, *. scr, *. bat, *. js e *. pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza è opportuno contattare l'Amministratore di sistema o l'Help Desk per una valutazione dei singoli casi.
11.8 - Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

11.9 - Nel caso fosse necessario inviare allegati “pesanti” (oltre ai 25 MB) è opportuno ricorrere alla compressione dei file originali in un archivio di formato. zip o equivalente e agli strumenti di pubblicazione di file disponibili nel sistema di posta. Per esigenze particolari, è consentito il ricorso agli strumenti cloud raggiungibili dalla rete dell’Ente, coerentemente a quanto disposto al punto 8. 9.
11.10 - Non è consentito l’invio automatico di e-mail all’indirizzo e-mail privato (attivando per esempio un “inoltro” automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un avviso di assenza facendo menzione di chi, all’interno dell’Ente, assumerà le mansioni durante l’assenza oppure indicando un indirizzo email alternativo preferibilmente di tipo condiviso. Si rammenta che ciascun utente ha il diritto alla disconnessione e il diritto di non dover presidiare la propria casella di posta elettronica nel periodo di ferie, poiché le stesse sono destinate al recupero psico-fisico delle energie (cfr. L. 81/2017).
11.11 - Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, dell’utente, qualora per necessità delle strutture si debba accedere alla sua casella di posta, il titolare della casella di posta ha la facoltà di delegare un altro utente, denominato “fiduciario”, per verificare il contenuto di messaggi e per inoltrare al Responsabile del servizio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. La delega si esprime attraverso l’apposita funzione presente sull’interfaccia della mail istituzionale.
11.12 - Nel caso non sia presente nemmeno il fiduciario, solo in casi di straordinaria necessità ed urgenza e per ragioni di sicurezza, il Responsabile del servizio a cui è assegnato l’utente assente potrà richiedere all’Amministratore di Sistema di accedere alla sua casella di posta. Sarà compito del Responsabile del servizio assicurarsi che sia redatto un verbale attestante quanto avvenuto e che venga informato il lavoratore interessato.
11.13 - La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, possibilmente su autorizzazione del Responsabile del servizio competente. Per evitare violazioni della privacy per diffusione degli indirizzi di posta nonché che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo e indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.
11.14 - È consentito inviare messaggi di posta elettronica in nome e per conto di un altro utente solo su sua espressa autorizzazione formale o delega.
11.15 - I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l’eliminazione dello spam. I messaggi contenenti virus riconosciuti vengono eliminati dal sistema.
11.16 - Nel caso in cui l’utente non presti più la sua attività lavorativa, la casella di posta elettronica nominativa sarà disattivata su segnalazione del Responsabile del servizio.
11.17 - Prima della cessazione dal servizio, l’utente è tenuto ad impostare una risposta automatica che informa di tale cessazione e indica un indirizzo mail alternativo, preferibilmente di gruppo, cui rivolgersi per le tematiche precedentemente trattate dall’utente stesso. Se per esigenze lavorative sorgesse la necessità di accedere al contenuto di tale casella di posta, il Responsabile del servizio a cui l’utente era assegnato potrà inoltrare motivata richiesta all'Amministratore di sistema.
11.19 - In coerenza con il punto 8. 8 non è prevista la possibilità di produrre copia delle caselle di posta per utenti non più in servizio presso l’Amministrazione. In ogni caso si informa che il contenuto delle caselle di posta elettronica cancellate potrà essere trattato dall’Ente, per il tramite dell’Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Le informazioni così raccolte saranno utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 “General Data Protection Regulation”. Si informa che, ai sensi della normativa sull’archiviazione e conservazione degli atti amministrativi, dell'articolo 2214 del Codice civile e dell'articolo 22 del Dpr 600/73, per ottemperare legittime istanze di accesso agli atti ai sensi della L. 241/90 o accesso civico generalizzato (d. lgs 33/13) l’Ente deve conservare per dieci anni sui propri Server di Posta Elettronica tutti i messaggi di posta elettronica aventi rilevanza istruttoria o inerenti l’attività procedimentale e contrattuale.

12 - Processo di abilitazione/disabilitazione alle procedure

12.1 - Il Responsabile del servizio determina per ogni dipendente assegnato alla struttura le abilitazioni e i profili da attribuire, modificare o revocare in coerenza con le funzioni e le singole attività per ciascuno di essi secondo le regole di liceità, correttezza e trasparenza, anche con riferimento alle corrette profilazioni sulla base del principio di accountability sancito dal Regolamento (UE) 2016/679. È richiesta pertanto ai responsabili dei servizi una costante verifica di tipo organizzativo sulla necessità e attualità delle abilitazioni in capo ai dipendenti assegnati alla propria struttura.
12.2 - I percorsi di abilitazione e disabilitazione devono essere "tracciabili" e veicolati, dall'Amministratore di Sistema, attraverso gli strumenti messi a disposizione, verso il "soggetto individuato". La responsabilità delle attribuzioni e delle mancate cancellazioni è una responsabilità del Responsabile del servizio.
12.3 - Ogni qualvolta il "soggetto individuato" abiliti un dipendente ad una procedura/applicativo con il relativo profilo, deve essere dato riscontro al Responsabile del servizio richiedente e al dipendente abilitato. Si intende per "soggetto individuato" chi detiene la possibilità di attribuire ruoli/profili alle persone rispetto agli applicativi: il ruolo può essere in capo all'Amministrazione di Sistema e/o a altri funzionari dell'Ente in relazione allo specifico applicativo.

13 - Utilizzo dei telefoni, kit di firma digitale, fotocopiatrici, scanner, tablet, pc e stampanti messi a disposizione dall'Ente.

13.1 - L'utente è consapevole che tutti gli strumenti dati in uso sono messi a disposizione dall'Ente per lo svolgimento dell'attività lavorativa.
13.2 - Qualora venisse assegnato un pc, tablet, smartphone o cellulare, o anche la sola SIM, all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari, smartphone e/o SIM dell'Ente si applicano, a compendio delle regole definite dall'Ufficio competente, le disposizioni sopra previste per gli altri dispositivi informatici e per l'accesso in rete, per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle indicazioni per la protezione dell'accesso al dispositivo e per il corretto uso della navigazione in Internet e della posta elettronica (cfr. punti 10 e 11).
13.3 - La stampa di documenti avviene, di norma, su dispositivi multifunzione disponibili all'interno della sede comunale e condivise mediante il dominio BORGHETTO. LOCAL.
13.4 - Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:
a) stampare documenti solo se strettamente necessario per lo svolgimento delle proprie funzioni operative tenuto conto del principio di dematerializzazione;
b) prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.
13.5 - Nei casi di telelavoro e lavoro agile non è prevista l'assegnazione di dispositivi di stampa individuali.
13.6 - Nel caso in cui si rendesse necessaria la stampa di informazioni riservate, l'utente dovrà utilizzare le apposite funzioni di stampa riservata, disponibili sui dispositivi multifunzione, per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.
13.7 - Non è consentita l'installazione di dispositivi di stampa di proprietà degli utenti sui PC messi a disposizione dall'Ente.
13.8 - Gli spazi di condivisione file server (on premise) o cloud, devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello spazio di condivisione apposito al fine di impedire la perdita di dati aziendali, a seguito di guasti alle PdL.
In caso di comprovato pericolo per la sicurezza dei sistemi, AgID potrà procedere alla rimozione di file e/o applicazioni presenti negli spazi di condivisione degli Utenti, dandone successiva e tempestiva comunicazione agli interessati.
13 9 - L'uso del kit di firma digitale, anche remota, è strettamente personale e non cedibile a terzi.

14 - Assistenza agli utenti e manutenzioni

14.1 - L'Amministratore di Sistema può accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

a) verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
b) verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
c) richieste di aggiornamento software e manutenzione preventiva hardware e software.

14.2 - Gli interventi tecnici possono avvenire previo consenso dell'utente quando l'intervento di che trattasi richiede l'accesso ad aree personali dell'utente stesso.
14.3 - L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.
14.4 - Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di sistema devono presenziare alla sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente documento.

15 - Log di sistema

15.1 - I log relativi all'uso del File System di dominio e della intranet, quelli relativi all'utilizzo di strumenti, reperibili nella memoria degli strumenti stessi ovvero sui server o sui router, nonché i file salvati o trattati su server o strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di sistema, per esigenze di servizio, per la sicurezza del lavoro e per la tutela del patrimonio, ovvero quando la verifica sia conseguente a specifiche richieste delle autorità competenti.
Le informazioni registrate nei log dipendono dalla natura degli eventi tracciati e dalle finalità associate. Devono almeno permettere di:

- imputare l'evento tracciato (azione o tentativo di azione sul sistema informatico) al proprio autore (persona fisica, attrezzatura tecnica, programma informatico, ecc.);
- datare l'evento (grazie alla sincronizzazione degli orologi di sistema);
- valutare l'evento in termini di: tipo di operazione (es. invio di una mail), parametri rilevanti dell'azione (es. destinatari della mail), risultato dell'operazione (es. successo o fallimento).

In nessun caso i messaggi di log possono contenere informazioni confidenziali come password o i corrispondenti hash, qualsiasi forma di autenticazione utente (es. chiavi pubbliche) o altra informazione la cui riservatezza deve essere preservata.
15.2 - I controlli possono avvenire secondo le disposizioni previste al successivo punto 16 del presente Regolamento.
15.3 - Le informazioni in possesso dell'Amministrazione comunale, di cui al comma 1, possono essere utilizzate esclusivamente per le finalità connesse al rapporto di lavoro e nei limiti stabiliti dal presente regolamento, con espresso divieto di qualunque forma di controllo sistematico o continuativo sull'utilizzo degli strumenti informatici da parte degli utenti.

16 - Controlli sugli strumenti informatici (art. 6. 1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

16. 1 - Poiché, in caso di violazioni contrattuali o normative, sia il datore di lavoro che il singolo lavoratore possono essere soggetti a sanzioni — anche di natura penale — l'Ente, nel rispetto dei vincoli previsti dall'ordinamento e dal contratto, procederà alla verifica del rispetto delle regole e della integrità del sistema informatico. Il datore di lavoro, esclusivamente per esigenze organizzative e produttive, per la sicurezza sul lavoro e per la tutela del patrimonio dell'Ente, può, previa stipula di accordo collettivo con la rappresentanza sindacale unitaria o le rappresentanze sindacali aziendali, avvalersi di sistemi che consentono, in conformità allo Statuto dei lavoratori (art. 4 della Legge n.

300/1970), forme indirette di controllo a distanza ("cd. controllo preterintenzionale") e comportano il trattamento di dati personali riferiti o riferibili ai lavoratori. Resta fermo l'obbligo di rispettare le procedure di informazione e consultazione dei lavoratori e delle organizzazioni sindacali, sia per l'introduzione o la modifica di sistemi automatizzati per la raccolta e l'utilizzo dei dati, sia per qualsiasi procedura tecnica destinata a monitorare movimenti o produttività dei lavoratori.
16.2 - I controlli devono essere effettuati nel pieno rispetto del presente regolamento e secondo i seguenti principi:

- proporzionalità: il controllo e la sua estensione devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite;
- trasparenza: l'adozione del regolamento mira a informare chiaramente gli utenti circa i diritti e i doveri di entrambe le parti;
- pertinenza e non eccedenza: evitando interferenze ingiustificate con i diritti e le libertà fondamentali dei lavoratori e contrastando controlli prolungati, costanti o indiscriminati.

16.3 - L'uso degli strumenti informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato al precedente punto 15 del presente documento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti ai punti 17 e 18) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti informatici.

17 - Controlli e monitoraggi

17.1 - L'Ente imposta la propria azione di monitoraggio e controllo sui sistemi informatici messi a disposizione per lo svolgimento dell'attività lavorativa nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli utenti, adottando in ogni caso soluzioni tecnologiche idonee a garantire la sicurezza dei sistemi informativi e dei dati gestiti. A tal fine, l'Ente utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti *file di log*, che consentono di tracciare eventuali anomalie o minacce informatiche in grado di compromettere la funzionalità e la sicurezza degli apparati informatici e delle informazioni trattate. I file di log relativi alla navigazione internet sono registrati e conservati per finalità di sicurezza in conformità alla normativa vigente e alle disposizioni interne adottate. In presenza di eventi anomali o pregiudizievoli per la sicurezza, tali file potranno essere esaminati dall' Amministratore di Sistema per l'individuazione dei problemi e l'adozione delle misure necessarie.
Tutte le attività di controllo e monitoraggio sono svolte nel rispetto del Codice dell'Amministrazione Digitale (CAD), della normativa in materia di tutela della libertà e dignità dei lavoratori e della disciplina europea e nazionale in materia di protezione dei dati personali.
L'Amministratore di Sistema, qualora rilevi anomalie o configurazioni non corrette delle postazioni di lavoro, può procedere a isolare immediatamente l'origine dell'anomalia, anche senza preavviso all'utente, al fine di salvaguardare la sicurezza e l'integrità dei sistemi informativi. In tali casi sarà successivamente fornita all'utente un'apposita informativa sui motivi dell'intervento.
17.2 - I dati registrati dai sistemi di monitoraggio possono essere aggregati ed elaborati per effettuare controlli finalizzati a prevenire abusi nell'uso delle risorse informatiche, verificare la sicurezza della rete comunale e individuare le cause di eventuali malfunzionamenti.
17.3 - I controlli sono effettuati dall'Amministratore di Sistema, che agisce secondo procedure strutturate, nel rispetto delle norme sulla protezione dei dati personali. In particolare:

- navigazione Internet: l'Amministratore di Sistema potrà visionare, tramite reportistica anonima ottenuta da software di analisi dei log in tempo reale, le tipologie di accesso (https, ftp ecc.), il numero di accessi, le pagine visualizzate, i volumi di traffico, le fasce orarie di utilizzo e i tentativi di intrusione verso la rete comunale o verso singole postazioni. posta elettronica: potrà essere analizzato il flusso dei messaggi inviati e ricevuti tramite l'indirizzo istituzionale,

limitatamente ai dati necessari a rilevare anomalie, errori di consegna/spedizione o eventi che possano pregiudicare la sicurezza o il corretto funzionamento del servizio di posta.

- rete interna: saranno verificati tentativi di intrusione o accesso non autorizzato a risorse protette (file, cartelle e servizi di rete). Potrà essere monitorato il numero complessivo di accessi, nonché ogni tentativo di accesso negato a risorse comunali protette.

Ogni abuso o utilizzo improprio del sistema informativo sarà segnalato ai competenti uffici.

17.4 - L'Amministratore di Sistema, su richiesta dell'Autorità Giudiziaria o delle Forze di Polizia, potrà fornire in qualsiasi momento i dati registrati dai sistemi di logging, nel rispetto della normativa vigente.

18 - Conservazione dei dati e dismissione apparecchiature informatiche

18.1 - In conformità agli articoli 5 e 6 del Regolamento (UE) 679/2016 e ai principi di legittimità, proporzionalità, sicurezza, accuratezza e corretta conservazione dei dati, si precisa quanto segue:

- Per la navigazione Internet non viene effettuata alcuna conservazione dei log; sono eseguiti esclusivamente controlli in tempo reale.
- I log degli Amministratori di Sistema**,** previsti dai requisiti minimi di sicurezza ICT, sono conservati dal fornitore incaricato mediante sistemi di conservazione certificata, secondo le tempistiche e le modalità tecniche definite dal relativo servizio.

18.2 - In casi eccezionali – ad esempio: per esigenze tecniche o di sicurezza o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

18.3 - L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

Le misure di sicurezza implementate per proteggere i log, da problemi operativi o modifiche non autorizzate (volontarie o involontarie) garantiscono:

- la correttezza dei messaggi di log, sottoponendo a controllo i meccanismi di generazione dei log per ogni sistema IT;
- l'integrità dei messaggi di log, mediante meccanismi di cifratura durante la trasmissione degli stessi dalla fonte alla piattaforma di centralizzazione;
- la disponibilità dei messaggi di log: grazie a meccanismi di *fault tolerance* relativi al dimensionamento della memoria delle fonti di log;
- l'inalterabilità e l'accesso autorizzato ai messaggi di log: secondo il principio di *segregation of duties* e tramite meccanismi di controllo accessi alla piattaforma;
- sul file system centralizzato, i log sono raccolti solo per la finalità di conservazione, secondo quanto stabilito dalle vigenti leggi;
- l'accesso è consentito solo alle PdL degli specialisti di sicurezza e con le credenziali dell'Amministratore di Sistema.

18.4 - I servizi 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 servizio stesso, il quale contemporaneamente attesterà la cancellazione dall' inventario patrimoniale. Secondo quanto previsto dalla normativa (GDPR, rifiuti di apparecchiature elettriche ed elettroniche, ecc.) e secondo le procedure previste. Solo successivamente il servizio CED provvederà al ritiro, alla predisposizione degli atti e delle operazioni per lo smaltimento.

18.5 - La dismissione e lo smaltimento dei dispositivi deve essere preceduta dalla rimozione delle memorie di archiviazione.

19 - Utilizzo dei Social Network

19.1 - L'utilizzo a fini promozionali e commerciali di strumenti di tipo "social media", dei blog e dei forum, anche professionali, è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive e istruzioni operative al personale addetto alla comunicazione attraverso gli account istituzionali.
19.2 - La partecipazione o consultazione dei social media durante l'orario di lavoro è consentita esclusivamente in casi di necessità lavorative o necessità di contatti attraverso messaggistica istantanea.
19.3 - Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.
19.4 - La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione.
19.5 - L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso scritto di questi, e comunque non potrà pubblicare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso scritto/esplicito del Responsabile del servizio di appartenenza, salvo in casi di manifestazioni pubbliche ad accesso libero.
19.6 - Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

20 - Sito Web istituzionale

20.1 - Al fine di garantire un'ampia, efficace ed efficiente divulgazione delle informazioni relative alle attività istituzionali del Comune di Borghetto Santo Spirito, è istituito il sito web istituzionale con nome a dominio **www.comune.borghettosantospirito.sv.it**
20.2 - La gestione tecnica del sito è affidata all'ufficio CED – Innovazione tecnologica, che provvede a:

- generare e rilasciare le credenziali di accesso al sistema di gestione dei contenuti (CMS);
- formare tecnicamente e supportare i soggetti incaricati dell'inserimento e dell'aggiornamento dei contenuti;
- gestire l'ordinaria amministrazione e la supervisione della struttura generale del sito, incluse le impostazioni delle pagine web.

20.3 - Il CED non è responsabile dei contenuti pubblicati sul sito né delle informazioni in esso presenti.
20.4 - La gestione dei contenuti pubblicati sul sito web istituzionale è demandata ai singoli uffici comunali, ciascuno per la propria area di competenza. Ogni Ufficio è responsabile dell'inserimento, dell'aggiornamento e della verifica delle informazioni relative alle attività, ai procedimenti e ai servizi di propria pertinenza, assicurandone la completezza, la correttezza e la conformità alle disposizioni normative vigenti.
A tal fine, il Servizio CED – Innovazione tecnologica fornisce un accesso riservato al sito a ciascun dipendente designato dal proprio Responsabile di servizio, che consente la pubblicazione autonoma di notizie, documenti, bandi e altre informazioni, definendo modalità, tempi e finestre di pubblicazione.

20.5 - Ogni Responsabile di Servizio può designare uno o più delegati incaricati degli aggiornamenti relativi al proprio settore.
20.6 - Il Responsabile o suo delegato è tenuto a:

a) operare nel pieno rispetto delle leggi e dei regolamenti vigenti;
b) effettuare le pubblicazioni secondo le modalità concordate con il CED;
c) non diffondere, salvo i casi consentiti dalla legge, dati sensibili o giudiziari;
d) evitare il collegamento a siti web ("link") che trattino argomenti non pertinenti alle finalità istituzionali del sito comunale o che possano, anche indirettamente, arrecare pregiudizio all'immagine dell'Ente.

21 - Comportamenti non consentiti

21.1 - Sono vietati a tutti gli utenti i seguenti comportamenti:

a) l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche e/o lo scambio di comunicazioni mediante falsa identità;
b) l'installazione, sulla PdL in dotazione, di software non coperto da licenza o, comunque, non preventivamente autorizzato;
c) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file utili al servizio/lavoro/ufficio e di ogni altra risorsa informatica;
d) l'allontanamento dalle PdL senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della PdL);
e) il mantenimento delle PdL accese al termine della giornata lavorativa;
f) la modifica delle configurazioni di base dei dispositivi assegnati dall'Ente senza l'autorizzazione preventiva dell'Amministratore di Sistema (non è possibile, ad esempio, configurare account privati nel client di posta);
g) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

22 - Protezione contro furti e danneggiamenti

22.1 - Tutte le PdL portatili e i dispositivi mobili devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in esse contenuti.
22.2 - L'Utente è tenuto a informare immediatamente il Responsabile del Servizio e il CED qualora vi sia la possibilità di una violazione di dati personali, di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

23 - Formazione e aggiornamento

23.1 - Il Comune di Borghetto Santo Spirito promuove, all'interno del piano annuale della formazione, l'aggiornamento e la formazione dei propri dipendenti in merito al corretto utilizzo delle strumentazioni informatiche e delle apparecchiature telefoniche.

24 - Responsabilità e sanzioni

24.1 - La violazione del presente documento e dei Codici di comportamento del personale può comportare l'applicazione delle sanzioni disciplinari previste dal decreto legislativo 30 marzo 2001, n. 165 e s. m. i., dai contratti collettivi applicabili al personale in servizio e dal singolo contratto di lavoro.

24.2 - Resta ferma la responsabilità civile, penale e contabile di ogni Utente per fatti illeciti e/o danni derivanti da usi non consentiti della rete o degli strumenti informatici messi a disposizione, anche alla luce delle prescrizioni contenute nel presente regolamento.
24.3 - Con riferimento ai collaboratori e al personale comunque estraneo all'Amministrazione. Qualora questi per l'espletamento dei rispettivi incarichi siano autorizzati a utilizzare gli strumenti elettronici considerati dal presente disciplinare, nell'ambito dei contratti e provvedimenti di conferimento dei relativi incarichi dovrà essere inserita un'espressa clausola che imponga l'obbligo in capo agli stessi lavoratori di rispettare il disciplinare in questione, con previsione del diritto del Comune, nei casi di violazione accertata di particolare gravità, di risolvere il contratto stesso, con salvezza di ogni eventuale azione civile e/o penale a carico del contraente inadempiente, laddove ne ricorrano i presupposti di legge.

25 - Pubblicazione e messa a disposizione

25.1 - La sua pubblicizzazione avverrà nelle seguenti forme: trasmissione per posta elettronica interna a tutti i Responsabili di servizio e a tutti gli utenti, attraverso la rete intranet del sito istituzionale.

26 – Aggiornamento delle disposizioni e delle regole

26.1 - 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.

27 – Glossario

Access Point	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 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.
Account	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: • 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	È 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.
Amministratori di sistema	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.

Antivirus	Programma in grado di riconoscere un virus presente in un file e di eliminarlo o di renderlo inoffensivo.
API	Un insieme di procedure (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito.
Apparati attivi	Apparecchiature hardware collegate alla rete che ne permettono il funzionamento (es. router, switch).
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 file.
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 multiplazione.
Backup	Procedura per la duplicazione dei dati su un supporto distinto da quello sul quale sono memorizzati, in modo da garantire 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.
BCC	Blind Carbon Copy: Campo delle e-mail che consente di aggiungere destinatari nascosti. I contatti inseriti in BCC ricevono il messaggio, ma non sono visibili agli altri destinatari (né in A né in CC), garantendo maggiore riservatezza.
BIOS	Basic Input/Output System: Firmware di base del computer che inizializza l'hardware all'avvio e gestisce il processo di boot. Può includere una password di protezione che blocca l'accesso al sistema prima del caricamento del sistema operativo.
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.
BYOD	Bring Your Own Device: modello organizzativo che consente ai dipendenti di utilizzare dispositivi personali — come laptop, smartphone e tablet — per accedere a risorse e servizi aziendali. Richiede policy dedicate per garantire sicurezza, conformità e tutela dei dati.
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.

Ccn	Nell'ambito della gestione delle e-mail indica informazioni, procedure o accorgimenti non formalizzati ma conosciuti solo da alcune persone — ad esempio modalità "di prassi" per gestire caselle condivise, regole informali di smistamento, criteri impliciti di priorità o tecniche personali per organizzare la posta.
CED	Centro Elaborazione Dati*:* struttura tecnica che gestisce, mantiene e protegge l'infrastruttura informatica dell'ente. Si occupa di server, reti, applicativi e supporto agli utenti.
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 software.

Cloud Computing	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. 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.
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. È 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 www.comune.XXX.it , 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 *comune.XXXXX.it*) è un nome di dominio. Essi vengono utilizzati in diversi contesti di rete e in ambito specifico per la denominazione o l'indirizzamento. 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".
Dominio Microsoft	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" 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.
Download	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.
E-mail	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.
File	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.
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 specificamente 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 indipendentemente dalla loro

	sottostante architettura hardware e software, garantendo così l'interoperabilità tra sistemi e sottoreti fisiche diverse.
Interoperabilità	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.
Intranet	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).
IP	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.
IPSEC	È 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.
LAN	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.
Logging	Attività di acquisizione cronologica di informazioni attinenti all'attività effettuata sui sistemi siano essi semplici apparati o servizi informatici.
Malware	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.
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.
PdL	(Postazione di Lavoro): Insieme di dotazioni informatiche assegnate a un dipendente: PC, monitor, periferiche, software e accessi necessari allo svolgimento delle attività operative.
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 "instradatore"), 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.
Sistema IT	L'insieme coordinato di tecnologie, infrastrutture, servizi digitali, applicativi e procedure che supportano le attività dell'ente. Comprende hardware, software, reti, sicurezza e gestione dei dati.
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 (fase 2).
SPCCloud	Sistema Pubblico di Connettività e cooperazione in cloud per l'erogazione di servizi a favore della Pubblica amministrazione.
SPID	Il 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	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. 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: • 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. In italiano un termine che potrebbe sostituire quello inglese è "sistema di archiviazione dati".
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. È 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	È 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; nello specifico corrompendo i file di sistema, sprecando le risorse, distruggendo i dati o creando 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.