Città di Novi Ligure

Regolamento interno per la sicurezza e la gestione degli strumenti informatici comunali

Esaminato dalla Giunta Comunale con parere favorevole per il successivo inoltro alla Commissione Consiliare nella seduta del 22 agosto 2019

Sommario

Allegato:
- Presa visione regolamento

1. DISPOSIZIONI GENERALI - Oggetto e ambito di applicazione

1. Il presente regolamento, nel rispetto delle norme vigenti, definisce un insieme di regole tecniche, organizzative e procedurali allo scopo di:

   a. disciplinare le modalità di accesso e di uso degli strumenti e delle risorse informatiche per il Comune di Novi Ligure;

   b. salvaguardare il patrimonio informativo del Comune di Novi Ligure costituito dall'insieme delle banche dati in formato digitale e da tutti i documenti prodotti tramite l'utilizzo di risorse informatiche, al fine di garantire l'integrità, la riservatezza e la disponibilità dei dati trattati e ridurne al minimo i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta come disciplinate da leggi e/o regolamenti;

   c. favorire l'individuazione di soluzioni atte a far fronte al problema della sicurezza informatica nel pieno rispetto della normativa sul GDPR (General Data Protection Regulation) e in ottemperanza alle misure minime di sicurezza ICT per la pubblica amministrazione e al piano triennale per l'informatica della pubblica amministrazione che potenzia, tra l'altro, il ruolo di CERT-PA (C*omputer Emergency Readiness/Response Team*);

   d. fornire uno strumento informativo a uso dei lavoratori;

   e. responsabilizzare l'utente nell'utilizzo dei sistemi informativi;

   f. gestire gli accessi esterni per il telelavoro e per le teleassistenze dei fornitori della PA.

2. DEFINIZIONI

Ai fini del presente regolamento s'intende per:

- **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; secondo le misure minime di sicurezza gli amministratori di sistema devono accedere con le proprie utenze amministrative e solo in casi particolari e documentati possono accedere con l'utenza Administrator generica;
- **Antivirus:** Programma in grado di riconoscere un virus presente in un file e di eliminarlo o di renderlo inoffensivo
- **Apparati attivi**: apparecchiature hardware collegate alla rete che ne permettono il funzionamento;
- **Aree condivise**: spazi di memorizzazione messi a disposizione degli utenti sui sistemi centralizzati per la condivisione e lo scambio di files;
- **Attachment**: (attaccamento) File allegato: può essere un allegato alla posta elettronica o a qualsiasi software di gestione dei file
- **Backup**: procedura per la duplicazione dei dati su un supporto esterno o distinto da quello sul quale sono memorizzati, in modo da garantirne una copia di riserva;
- **Banda**: Quantità di dati per unità di tempo che può viaggiare su una connessione. Nella banda ampia la velocità varia da 64 Kbps a 1,544 Mbps. Nella banda larga la comunicazione avviene a velocità superiori a 1,544 Mbps.
- **CAD:** Codice dell'amministrazione digitale: norma che riunisce in sé diverse norme emanate tra il 1997 e il 2005 riguardanti l'informatizzazione della pubblica amministrazione, ed in particolare il documento informatico, la firma elettronica e la firma digitale, delle quali stabilisce l'equivalenza con il documento cartaceo e con la firma autografa.
- **CERT_PA:** opera all'interno di AgID e ha il compito di supportare le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica
- **CONSIP:** è la centrale acquisti della pubblica amministrazione italiana; è una società per azioni il cui unico azionista è il Ministero dell'economia e delle finanze del governo italiano ed opera nell'esclusivo interesse dello Stato
- **Cookie:** Tradotto letteralmente significa biscotto. E' un file memorizzato sul proprio computer che identifica il computer quando è collegato ad alcuni siti Internet.
- **Cloud:** indica un paradigma di erogazione di servizi offerti on demand da un fornitore ad un cliente finale attraverso la rete Internet
- **Data breach**: incidente di sicurezza in cui dati sensibili, riservati, protetti vengono consultati, copiati, trasmessi, rubati o utilizzati da soggetti non autorizzati
- **Dati personali:** dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale, dati inerenti lo stile di vita la situazione economica,

finanziaria, patrimoniale, fiscale, dati di connessione: indirizzo IP, login, altro, dati di localizzazione: ubicazione, GPS, GSM, altro.

- **DNS (Domain Name System):** Sistema che gestisce gli indirizzi dei domini Internet.
- **DPIA - Data Protection Impact Assessment" - "Valutazione d'impatto sulla protezione dei dati":** è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.
- **Ente:** il Comune di Novi Ligure
- **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 comunale e contribuisce alla sicurezza della rete stessa.
- **Garante Privacy:** il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.
- **Indirizzamento**: attività di assegnazione di indirizzi logici 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;
- **IP:** Indirizzo che permette di identificare in modo univoco un computer collegato in rete. Si suddivide in due parti, la prima individua la rete dove si trova il computer, la seconda individua il computer all'interno di quella rete.
- **Interoperabilita:** 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;
- **Linee guida o policy**: regole operative tecniche e/o organizzative atte a guidare i processi lavorativi, decisionali e attuativi;
- **Log**: file che registra attività di base quali l'accesso ai computer e che è presente sui server della rete informatica
- **Logging**: attività di acquisizione cronologica di informazioni attinenti all'attività effettuata sui sistemi siano essi semplici apparati o servizi informatici;
- **Misure minime di sicurezza**: le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle 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 consentire agli utenti di accedere e condividere una memoria di massa, in pratica costituita da uno o più dischi rigidi, all'interno della propria rete. In ambiente NetApp tale dispositivo prende il nome di FAS.
- **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
- **PagoPA**: é un sistema di pagamenti elettronici realizzato per rendere più semplice, sicuro e trasparente qualsiasi pagamento verso la Pubblica Amministrazione.
- **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;
- **Postazione di lavoro:** dispositivo (personal computer, notebook, thin/fat client, ecc.) che consente l'accesso al proprio ambiente di lavoro informatico;

- **Protocollo**: insieme di regole che definisce il formato dei messaggi scambiati tra due unità informatiche e che consente loro di comunicare nonché di comprendere la comunicazione;
- **Responsabile del trattamento:** il Dirigente/Responsabile P.O., oppure il soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.
- **Responsabile per la protezione dati – RPD o DPO:** il dipendente della struttura organizzativa del Comune, il professionista privato o impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento.
- **Registri delle attività di trattamento:** elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze.
- **Rete dati**: insieme dell'infrastruttura passiva (cavi, prese, ecc.) e degli apparati attivi (modem, router, ecc.) necessari alla interconnessione di apparati informatici;
- **SPC**: Sistema Pubblico di Connettività (SPC) 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
- **Titolare del trattamento:** l'autorità pubblica (il Comune o altro ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali
- **URL (Uniform Resource Locator):** Identifica in modo univoco le informazioni presenti su Internet, un indirizzo dal quale si richiamano le informazioni.
- **Utente:** persona fisica autorizzata ad accedere ai servizi informatici dell'Ente.
- **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

3. DESTINATARI

1. Il presente regolamento si applica a tutti gli utenti interni ed esterni.

2. Per utenti interni si intendono gli amministratori, i dipendenti a tempo indeterminato e a tempo determinato, nonché i collaboratori o altri soggetti opportunamente autorizzati che operano in via continuativa all'interno della rete comunale dell'ente.

3. Per utenti esterni si intendono:
   a. addetti delle ditte fornitrici di software che dovranno effettuare attività di manutenzione, limitatamente alle attività di loro competenza;
   b. dipendenti di enti esterni autorizzati all'accesso a specifiche banche dati e/o applicativi e/o documenti da apposite convenzioni, con le modalità stabilite dalle stesse;
   c. soggetti che, a fronte di particolari rapporti con l'Ente, abbiano la necessità di accedere alla rete dati interna per un periodo di tempo limitato (a titolo di esempio: studenti in stage/tirocinio, volontari espletanti il Servizio Civile Nazionale, consulenti, personale di cooperative, ecc.).

4. SOGGETTI AUTORIZZATI

1. L'Ente promuove l'utilizzo delle risorse informatiche, di Internet e della posta elettronica quali strumenti utili a perseguire le proprie finalità istituzionali. Di conseguenza, l'accesso alla rete dati comunale, nonché ai servizi da essa erogati, è consentito in relazione all'espletamento delle mansioni assegnate ovvero in correlazione all'attività cui gli utenti siano contrattualmente o istituzionalmente tenuti.

2. Tutti gli utenti, a cui vengono forniti accessi al sistema informatico, dovranno essere previamente autorizzati dalla struttura competente e attenersi scrupolosamente al presente regolamento.

5. PRINCIPI GENERALI

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzo di dati personali o di dati identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

2. Ciascun utente deve operare nel rispetto delle disposizioni contenute nel GDPR (regolamento (UE) n. 2016/679) nonché dei correlati regolamenti adottati in materia; in riferimento anche al codice di comportamento dei dipendenti delle pubbliche amministrazioni è responsabile del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati con essi trattati.

3. I trattamenti devono essere effettuati per finalità determinate, esplicite, lecite e legittime, osservando il principio di pertinenza e non eccedenza. I dati devono essere trattati nella misura meno invasiva possibile. Le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere mirate all'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza personale, ovvero degli atti d'Ufficio.

4. L'ente si impegna a rispettare il principio del "once only" evitando di chiedere a cittadini e imprese informazioni già fornite.

5. Gli acquisti di materiale informatico sono effettuati dall'Ufficio coordinamento e sviluppo informatico che ne cura anche la parte manutentiva per quanto di competenza.

6. L' Ufficio coordinamento e sviluppo informatico si impegna a perseguire un'adeguata e funzionale evoluzione dei sistemi informatici promuovendo la sostituzione di quelli non adeguati alle misure minime di sicurezza e l'adozione di nuove soluzioni a sostegno dell'attività lavorativa.

7. Il personal computer (fisso o mobile) ed i relativi programmi e applicazioni affidati al dipendente sono strumenti di lavoro e ogni utilizzo non inerente all'attività lavorativa è vietato. L'utilizzo improprio, inoltre, può provocare disservizi, costi di manutenzione aggiuntivi e minacce alla sicurezza e pertanto:

   a) le attrezzature informatiche vanno custodite in modo appropriato ed utilizzate esclusivamente per le attività lavorative cui ciascun assegnatario è preposto. Le condotte non conformi comportano responsabilità disciplinare, fatte salve le azioni di rivalsa per eventuali danni arrecati e le responsabilità penali;

   b) le attrezzature informatiche non possono essere autonomamente spostate o trasferite poiché l'assegnazione all'utente della postazione di lavoro è registrata;

   c) il furto, il danneggiamento o lo smarrimento di attrezzature informatiche deve essere prontamente segnalato all'Ufficio Coordinamento e Sviluppo Informatico;

   d) non è consentito spostare o copiare su qualunque dispositivo elettronico personale documenti o files inerenti all'attività lavorativa e non è consentito scaricare files contenuti in supporti di memorizzazione non aventi alcuna attinenza con la propria prestazione lavorativa;

   e) l'Ente è tenuto a comunicare i log file contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle autorità competenti quando richiesto ai sensi di legge. Le eventuali attività di monitoraggio relative alle attività di navigazione e di utilizzo degli strumenti informatici, al fine di prevenire utilizzi indebiti degli strumenti stessi, che possono essere fonte di responsabilità per l'Ente, saranno svolte con l'autorizzazione del Segretario Generale e da soggetti a ciò preposti e saranno strettamente mirate all'area di rischio individuata;

   f) Il personal computer deve essere spento (salvo specifiche esigenze tecniche asseverate dal proprio Responsabile) o bloccato ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo.

6. STRUTTURA ORGANIZZATIVA

1. L'Ufficio coordinamento e sviluppo informatico ha il compito di:

- attuare, mantenere ed aggiornare il presente regolamento di gestione della sicurezza informatica e dell'utilizzo della struttura e dell'utilizzo dei mezzi informatici;
- gestire l'infrastruttura di rete dati e fonia della rete informatica comunale con particolare attenzione alla rete SPC;
- coordinare l'attività di comunicazione riguardante gli eventi relativi alle reti dati, ai servizi disponibili e alle problematiche di sicurezza e agli aggiornamenti software;
- monitorare la raccolta delle segnalazioni da parte degli utenti o dei software relativi concernenti eventuali problemi di sicurezza occorsi;
- gestire il sistema di posta elettronica e internet;
- coordinare e mantenere aggiornati i sistemi di comunicazione per il cittadino riguardanti i siti internet, le app, i social e ogni altro mezzo di divulgazione informatica;
- effettuare, mantenere e controllare i backup con attenzione alle attività di disaster recovery e continuazione del servizio pubblico;
- aggiornare e mantenere in sicurezza i sistemi operativi dei server e delle singole postazioni in ottemperanza alle misure minime di sicurezza;
- mantenere aggiornati ed efficienti i sistemi di antivirus e antispam;
- gestire il sistema documentale informatico e la conservazione digitale dei documenti informatici;
- interfacciarsi con i fornitori di software e di programmi per la risoluzione di problematiche informatiche e per l'acquisto di tecnologia informatica;
- provvedere al sostentamento e all'aggiornamento del parco informatico comunale e predisporre le postazioni di lavoro con le configurazioni e le policy adatte all'utente destinatario della risorsa informatica;
- presiedere a qualunque attività che riguardi l'informatica comunale e la gestione della fonia sia analogica che voip.

7. GESTIONE DELLA RETE DATI

1. La gestione delle reti dati consiste nella manutenzione dell'infrastruttura attiva e nel suo adeguamento tecnologico e funzionale, al fine di garantirne l'operatività.

2. L'Ente ha aderito al contratto quadro SPC2 della convenzione Consip secondo le normative AGID ed ha una infrastruttura con un centro stella situato presso l'Ufficio coordinamento e sviluppo informatico.

3. L'assegnazione dell'indirizzamento per gli apparati attivi collegati alla rete dati è a carico dell'Ufficio coordinamento e sviluppo informatico.

4. L'estensione della rete dati deve essere valutata tecnicamente dall'Ufficio coordinamento e sviluppo informatico e approvata dagli organi politici competenti.

5. Le modalità di accesso e autenticazione alle reti WiFi si dividono in modalità pubblica e privata.

- Per modalità pubblica si intendono le reti Wifi presenti in alcune zone esterne della città per l'accesso a tempo limitato e previa registrazione di utenti esterni. Vengono gestiti da un fornitore esterno
- Per modalità privata si intendono le reti wireless direttamente collegate alla rete informatica comunale. Possono accedere solo dispositivi autorizzati e appartenenti al parco informatico dell'ente.

6. È consentito l'accesso alla rete dati comunale per motivi lavorativi esclusivamente tramite modalità concordate e monitorate dall'Ufficio coordinamento e sviluppo informatico

7. È vietato l'utilizzo di qualsiasi apparato che possa costituire un punto di accesso esterno alla rete diverso da quelli gestiti dall'Ufficio coordinamento e sviluppo informatico

8. Da un punto di vista tecnico i computer appartengono ad un dominio gestito dai tre server centralizzati che assegnano indirizzi univoci e dinamici all'accesso della rete. Esistono altre apparecchiature informatiche che hanno assegnati un IP statico gestito dall'Ufficio coordinamento e sviluppo informatico.

9. Presso la biblioteca civica esiste, in parallelo con la rete dati comunale, una rete dati fornita e gestita dal CSI Piemonte nell'ambito del sistema pubblico bibliotecario regionale piemontese. A tale rete, totalmente distinta dalla rete comunale hanno accesso 9 postazioni della biblioteca.

10. Presso la sede della Polizia Municipale è stata installata una rete parallela SPC2 non accessibile dal dominio comunale per la gestione dei varchi, della ZTL per il controllo della videosorveglianza e per la sala "com" della protezione civile.

8. AGGIORNAMENTI

1. Per mantenere i sistemi aggiornati e adeguati alle normative sia in termine di sicurezza che di operatività l'Ufficio coordinamento e sviluppo informatico opera in questi termini:

- Aggiornamenti di sistema o patch dei sistemi operativi: vengono installati durante la pausa pranzo oppure durante il blocco degli aggiornamenti del software operativo oppure in tarda serata lavorativa; in casi eccezionali possono avvenire durante l'orario lavorativo di sportello previo avvertimento.
- Aggiornamento delle procedure software per l'operatività dei servizi comunali: vengono effettuati una volta alla settimana previa comunicazione e durano circa un'ora. Prevedono un blocco delle operatività per quel che riguarda l'utilizzo delle procedure stesse. Capita a volte di fare aggiornamenti anche più volte durante la settimana.
- Aggiornamento dei sistemi operativi delle singole postazioni: vengono inviati in maniera silente tramite un applicativo centralizzato di antivirus che gestisce questo aspetto; l'utente viene avvertito tramite comunicazione prima dell'intervento. A volte si interviene manualmente in caso di blocco o di aggiornamenti particolari

- Aggiornamento dell'antivirus: sia l'aggiornamento dell'applicativo dell'antivirus che della definizione degli aggiornamenti sono gestiti direttamente e in maniera automatica dall'antivirus centralizzato
- Aggiornamenti di procedure particolari: vengono gestite in assistenza remota sul pc oggetto dell'aggiornamento direttamente dal personale dell'Ufficio

9. ASSISTENZA REMOTA

1. L'Ufficio coordinamento e sviluppo informatico in fase di predisposizione del personal computer dell'utente installa un software per il controllo remoto. Si tratta di un software con licenza free sia per uso personale che commerciale.

2. Il software (https://www.tightvnc.com/) prevede una parte configurabile che garantisce all'utente di approvare o meno la connessione da parte dell'Ufficio coordinamento e sviluppo informatico garantendo la privacy dell'interessato.

3. Viene utilizzato per effettuare aggiornamenti di sistema o di software, per monitorare e controllare comportamenti del pc e per ogni altra problematica legata all'utilizzo del computer.
4. Esiste una modalità utilizzata per la gestione e la condivisione del desktop anche tra utenti non amministratori. Per abilitarla è necessario contattare l'ufficio coordinamento e sviluppo informatico che permetterà tramite una password condivisa tra utenti la gestione del desktop in lettura.

10. CREAZIONE E GESTIONE DELLE CREDENZIALI

1. L'Ufficio coordinamento e sviluppo informatico genera le credenziali di autenticazione per l'accesso alla rete interna degli utenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (*userid*) associato a una parola chiave (*password*) riservata e conosciuta solamente dal medesimo
3. Ogni utente deve essere dotato di credenziali di autenticazione che corrispondono al criterio cognome e inziale del nome (ad esempio Mario Rossi = rossim); in materia di protezione dei dati personali, ogni utente è responsabile della gestione e conservazione delle proprie credenziali, assicurando la segretezza della componente riservata e la diligente custodia dei dispositivi in suo possesso e uso esclusivo.
4. La gestione delle credenziali di autenticazione inutilizzate ovvero la loro disattivazione è attuata nel rispetto dei tempi e dei modi definiti dalla vigente normativa in materia di protezione dei dati personali.
5. Il responsabile del trattamento deve comunicare all'Ufficio coordinamento e sviluppo informatico la perdita della qualità che consente all'utente/incaricato l'accesso ai dati, al fine di consentire la disattivazione delle credenziali di autenticazione assegnate.
6. L'Ufficio personale comunica periodicamente le modifiche dell'organico dell'ente per consentire la tempestiva gestione delle credenziali (creazione, disattivazione, eliminazione, variazione).

7. Esistono alcune postazioni che, in maniera del tutto eccezionale e per motivi di rotazione continuo del personale, (ad esempio sportello dell'anagrafe) in accordo con il segretario generale, gestiscono in maniera collettiva le postazioni, senza un utenza nominale. Rimangono invariate le credenziali di accesso personali dell'utenza sulle procedure, garantendo in tal modo l'autenticazione dell'utente che opera sulla macchina.

11. CRITERI DI SICUREZZA PER LA GESTIONE E LA PROTEZIONE DELLE PASSWORD

1. La password deve rispondere ai criteri di lunghezza, complessità e segretezza secondo queste specifiche:
- Lunghezza minima 8 caratteri
- Deve contenere almeno un numero
- Deve contenere almeno un segno di punteggiatura oppure una maiuscola
- Non deve essere uguale alla precedente o iniziare come la precedente
- Non può essere il nome utente e/o il nome del dispositivo (cioè il nome del computer o dell'Ufficio compresa la dicitura Comune di Novi Ligure).

2. Le password usate per accedere ai servizi degli Enti sono individuali e non devono essere utilizzate in altri contesti al di fuori dell'attività lavorativa.
3. La password deve essere conservata con la massima cura e diligenza: non deve essere condivisa con altri soggetti, non deve essere divulgata a voce o per telefono, né inviata tramite messaggio di posta elettronica; non deve inoltre essere memorizzata sul computer in forma leggibile.
4. Il sistema richiederà in automatico il cambio password dopo 180 giorni
5. Per motivi di privacy l'Ufficio coordinamento e sviluppo informatico non è a conoscenza delle password inserite dall'utente e quindi in caso di dimenticanza sarà necessario resettarla ed inserirla una nuova.
6. Qualora l'utente prenda coscienza che taluno può aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente cambiarla;

12. CRITERI DI SICUREZZA PER L'USO DEI DISPOSITIVI DI FIRMA DIGITALE E CNS

1. I titolari di smart card, business key e altri dispositivi per il riconoscimento che contengono certificati di firma e/o autenticazione (utilizzabili, per esempio, nei procedimenti amministrativi dell'Ente) sono responsabili del corretto utilizzo e devono custodire adeguatamente i dispositivi, il relativo PIN e tutto il materiale a corredo.
2. In caso di smarrimento del dispositivo ne deve essere fatta tempestiva denuncia alle forze dell'ordine.
3. Per la sua particolare funzione il dispositivo è strettamente personale.

13. ATTIVITA' DI LOGGING

1. L'Ufficio coordinamento e sviluppo informatico provvede ad effettuare attività di logging e monitoraggio dei sistemi:
    - Degli apparati attivi delle reti dati o comunque di quelli ritenuti strategici;
    - Dei sistemi di sicurezza installati a protezione delle reti stesse;
    - Dei servizi centralizzati fruibili attraverso una connessione alle reti;
    - Degli accessi da parte degli amministratori di sistema e dei telelavoristi;
    - Tracciando i tentativi di accesso degli utenti alla rete informatica comunale;

2. L'attività di logging viene condotta attraverso sistemi automatizzati ed ha finalità prevalentemente manutentiva, diagnostica e di rendicontazione. I log contengono dati sintetici tesi a garantire la sicurezza dei sistemi e degli applicativi e non riproducono pedissequamente sessioni di lavoro.

3. Le informazioni acquisite sono di natura tecnica e individuale; l'Ufficio coordinamento e sviluppo informatico utilizza tali informazioni per le attività di cui al precedente comma 2 e cura che le stesse non siano disponibili ad altri, se non nei limiti e nel rispetto delle modalità previste dalla vigente normativa sulla tutela dei dati personali e del presente regolamento.

4. Attraverso il firewall di rete perimetrale vengono monitorate le connessioni da e per la rete informatica comunale e gli accessi ad internet compresi le macro-aggregazioni (domini) dei siti visitati e bloccati.

5. Il periodo di conservazione dei file di log è di 180 giorni ma può variare a seconda delle necessità e dell'utilizzo degli stessi.

14. DISPONIBILITA' DEI DATI

1. L'Ufficio coordinamento e sviluppo informatico garantisce la disponibilità dei dati e opera con i dovuti privilegi di accesso e modifica, anche esclusivi, al fine di assicurarne la fruizione.
2. In caso di assenza improvvisa prolungata o impedimento dell'incaricato del trattamento, per esclusive necessità di operatività o di sicurezza del sistema, il responsabile del trattamento richiede all'Ufficio coordinamento e sviluppo informatico l'abilitazione all'accesso ai dati senza necessità di ricorrere all'utilizzo delle credenziali di autenticazione individualmente associate all'incaricato assente (emissione di nuova utenza o modifica di abilitazioni esistenti).
3. In caso di prolungata assenza o impedimento dell'utente, per esclusive necessità di operatività o di sicurezza del sistema, il superiore diretto richiede all'Ufficio coordinamento e sviluppo informatico l'abilitazione all'accesso ai dati dell'utente (utilizzo delle credenziali dell'utente o di parte delle stesse). In questo caso sarà cura del superiore diretto informare l'utente alla prima occasione utile.
4. Il comma 2 si applica anche agli incaricati del trattamento qualora con le modalità previste al comma 1 non sia possibile garantire l'operatività o la sicurezza.
5. I dati e i documenti informatici sono memorizzati in database centralizzati e/o aree appositamente creare per la memorizzazione ridondata. L'utente per salvaguardare il dato informatico deve salvare i documenti in queste aree e non sul proprio pc dove può rimanere

una copia dello stesso. L'Ufficio coordinamento e sviluppo informatico non garantisce il recupero dei dati informatici presenti sul disco rigido del pc (e quindi non sulle apposite aree condivise – vedi articolo 17) in caso di rottura del disco stesso.

15. MODALITA' DI UTILIZZO DI INTERNET

1. L'accesso a Internet è consentito a tutti gli utenti interni, debitamente autorizzati, e in conformità a quanto prescritto dall'art. 4 del presente regolamento.
2. Nell'utilizzo di Internet non sono consentite attività estranee alle proprie mansioni lavorative o compiti istituzionali o d'Ufficio. Non sono altresì consentite attività atte a violare il diritto d'autore, a degradare le performance delle reti dati della rete informatica comunale né ogni altra attività che possa ledere all'immagine dell'Ente.
3. L'accesso a internet è profilato in diverse categorie a seconda dell'utilizzo richiesto.
4. Il firewall gestisce e categorizza i siti internet in base ad informazioni di sicurezza informatica internazionale e l'Ufficio coordinamento e sviluppo informatico inibisce l'accesso alle categorie di siti che non sono per uso lavorativo; eventuali sblocchi di siti vengono gestiti singolarmente dietro richiesta dell'utente e verifica da parte dell'Ufficio stesso.
5. Come specificato nell'art. 13 vengono monitorati e loggati i collegamenti per macro aree e prodotto un report giornaliero sull'utilizzo di internet e delle connessioni in rete che transitano dal firewall. Tale report è utilizzato dall'Ufficio coordinamento e sviluppo informatico allo scopo di monitorare la rete e la sua sicurezza, preservando la privacy dell'utente.

16. MODALITA' DI UTILIZZO DELLA POSTA ELETTRONICA

1. L'Ufficio coordinamento e sviluppo informatico fornisce l'accesso a servizi di posta elettronica al fine dell'espletamento dell'attività lavorativa e istituzionale.
2. L'utente abilitato all'utilizzo della posta elettronica è in possesso di un indirizzo nominativo e di un indirizzo dell'Ufficio. L'indirizzo nominativo è presente solo sul computer dell'utente e viene ricevuta e inviata posta solo per quel pc mentre l'indirizzo dell'Ufficio viene utilizzati da tutti gli utenti dell'Ufficio oltre che dallo stesso utente. Ad esempio l'utente Mario Rossi dell'Ufficio personale avrà un indirizzo di posta m.rossi@comune.noviligure.al.it e un indirizzo dell'Ufficio personale@comune.noviligure.al.it.
3. In alcuni casi, vedi art. 10 punto 7, la postazione potrebbe essere sprovvista di posta elettronica o avere solo la posta generica dell'Ufficio.
4. Allo stato attuale sono due i server di posta elettronica che gestiscono la corrispondenza. Uno che contiene la maggior parte delle caselle di posta è un prodotto open source con sistema operativo Linux. L'altro che contiene una ventina di caselle di posta è invece un programma professionale e consente la visione della posta elettronica su più dispositivi.
5. Le caselle di posta elettronica dell'ambiente open source hanno una determinata dimensione su disco e terminato lo spazio su disco l'email viene rigettata producendo un messaggio di errore. Questo può accadere in casi di assenze prolungate ove le email continuano ad arrivare senza però essere scaricate dall'utente.

6. Non è consentito l'uso del sistema di posta elettronica per l'invio/ricezione di messaggi esclusivamente personali o altre attività non attinenti ai fini istituzionali del Comune, né l'invio di catene di messaggi di qualsiasi natura.
7. Gli utenti non devono inviare dati e informazioni classificate come sensibili o riservate con il sistema di posta elettronica in quanto, allo stato attuale la tecnologia non consente di garantire la totale riservatezza delle informazioni trasmesse.
8. È cura dell'utente gestire con continuità il contenuto della propria casella eliminando i propri messaggi in funzione anche delle indicazioni fornite dall'Ufficio coordinamento e sviluppo informatico. Come indicato nel punto 3 lo spazio su disco per ogni casella di posta è delimitato e quindi la posta in eccesso va eliminata.
9. La posta elettronica dei consiglieri, che non hanno una postazione informatica all'interno della rete informatica comunale, viene gestita creando un indirizzo riferito alla persona del consigliere con dominio del Comune e re-inoltrata direttamente alla casella di posta personale del consigliere.

17. AREE CONDIVISE

1. È responsabilità di tutti gli utenti interni, le cui postazioni siano opportunamente configurate, salvare i dati nelle aree condivise sui sistemi centralizzati come specificato nell'articolo 14 comma 5.
2. I dati salvati nelle aree condivise devono essere attinenti esclusivamente alla propria attività lavorativa.
3. È facoltà dell'Ufficio coordinamento e sviluppo informatico impostare dei limiti (*quote*) alla quantità di dati memorizzabili da parte dei singoli utenti in funzione delle risorse hardware disponibili nonché verificare il corretto uso dello spazio di memorizzazione analizzando a campione il formato dei file presenti nelle aree condivise e segnalando agli utenti la necessità di rimuovere situazioni anomale eventualmente riscontrate.
4. Esiste un'area condivisa accessibile a tutti gli utenti denominata "Scambio files" dove è possibile inserire e recuperare file o cartelle. Questo spazio deve essere utilizzato solo per lo scambio di files informatici e non per memorizzare in maniera permanente dati. Al termine dell'operazione di scambio è necessario cancellare il file o la cartella condivisa. E' facoltà dell'Ufficio coordinamento e sviluppo informatico eliminare tutto il contenuto della cartella.
5. I files e le cartelle devono essere memorizzate negli appositi spazi condivisi adoperando semplici regole di buon senso come ad esempio non creare troppe cartelle annidate, non utilizzare nomi troppo lunghi, non usare caratteri di punteggiatura nei nomi dei files, evitare di ridondare memorizzando più volte lo stesso file. Senza tali accorgimenti le operazioni di backup ma soprattutto di un eventuale recupero potrebbero essere difficoltose se non impossibili.

18. BACKUP E CONSERVAZIONE

1. L'Ufficio e coordinamento sviluppo informatico ha ricevuto l'approvazione del piano di continuità operativa e disaster recovery da Agid e presso la sede di Palazzo Pallavicini ha un server di dominio e un apparato per la ridondanza dei dati
2. Un altro apparato ridondato è presente presso la sede della Polizia Municipale.

3. I backup vengono eseguiti a livello centrale sui server virtuali secondo questa impostazione descritta anche nel documento delle misure minime di sicurezza:

- Tramite software di backup delle macchine virtuali viene effettuato giornalmente il backup delle configurazioni di sistema e dei principali server e settimanalmente quello dei server meno importanti. Esiste un software di backup su tape che settimanalmente effettua un backup. I dati degli utenti e le principali configurazioni/documenti importanti risiedono su Fas e su Nas entrambe compresi nel backup. Le nas sono inoltre ridondate.
- Più specificatamente i backup sono copiati su una Nas secondaria e i tape sono posizionati su una cassetta ignifuga ad una distanza di 100 metri in linea d'aria dal locale del ced e in una stanza non accessibile al pubblico.
- Tutti i backup sono criptati sia su nas che su tape.

4. Il recupero dei file avviene su richiesta dell'utente tramite lo stesso software che si occupa del backup.
5. La conservazione è l'attività volta a proteggere e custodire nel tempo gli archivi di documenti e dati informatici. Il sistema di conservazione, come previsto dall'art.44 del CAD, garantisce autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici. Sarà cura dell'Ufficio coordinamento e sviluppo informatico, di concerto con il dirigente preposto alla conservazione, utilizzare il software idoneo per la conservazione a norma dei documenti digitali dell'ente.

19. POSTAZIONI DI LAVORO

1. La postazione di lavoro affidata all'utente è uno strumento di lavoro; come tale deve essere custodita in modo appropriato e utilizzata solo per fini lavorativi. Ogni utilizzo non inerente all'attività lavorativa o istituzionale può contribuire a innescare disservizi, costi e minacce alla sicurezza informatica.
2. Per policy non è consentito installare autonomamente software o periferiche hardware e tutte le richieste saranno vagliate dall'Ufficio coordinamento e sviluppo informatico.
3. Non è consentito trasferire, sulla propria postazione di lavoro o sui server, file non aventi alcuna attinenza con la propria prestazione lavorativa.
4. L'antivirus lavora su tutte le postazioni e analizza in maniera diretta o indiretta tutti i files scaricati o creati sul computer.
5. La postazione di lavoro deve essere spenta correttamente prima di lasciare l'Ufficio o in caso di assenza prolungata. Lasciare una postazione di lavoro incustodita connessa alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.
6. L'Ufficio coordinamento e sviluppo informatico provvede al passaggio di computer tra un utente ed un altro salvando eventuali files e riproponendo il computer con le impostazioni predefinite
7. Il personal computer viene fornito all'utente con delle impostazioni standard che riguardano l'installazione di software lavorativi sia con licenza open che proprietaria, con le configurazioni necessarie all'accesso al protocollo informatico, alla posta elettronica e a internet.

20. TELELAVORO

1. Il telelavoro avviene attraverso un portatile, fornito dall'Ufficio coordinamento e sviluppo informatico agli utenti che ne hanno diritto, all'interno del quale è installato un software che dialoga con il firewall di rete attraverso una connessione VPN permettendo di accedere all'interno della rete comunale stessa.
2. La connessione permette il collegamento e passaggio di informazioni in maniera protetta e sicura e consente di lavorare dalla postazione fissa dell'Ufficio che quindi deve rimanere accesa.
3. Non è possibile altra forma di collegamento al di fuori di quella citata nei commi 1 e 2 e non è quindi permesso un collegamento con propri dispositivi.
4. Durante la connessione alla vpn il portatile è disabilitato all'accesso a internet.
5. Anche il portatile usato per il collegamento ha installato l'antivirus e quindi tutti gli eventuali passaggi di files dall'esterno all'interno o viceversa sono controllati dai due antivirus oltre che dal firewall di rete.

21. SUPPORTI REMOVIBILI

1. Sui dispositivi removibili non è permessa l'esecuzione automatica dei contenuti al momento della connessione come da misure minime di sicurezza.

22. CLOUD

1. L'Ufficio coordinamento e sviluppo informatico, aderendo alla recente normativa emanata da AGID in particolare con le circolari AgID n.2 e n. 3 del 9 aprile 2018, ha iniziato il processo di migrazione ai servizi cloud.

2. In particolare sono attivi diversi servizi in cloud quali il servizio di conservazione digitale dei documenti con un fornitore accreditato AGID, alcuni servizi di PagoPa, il servizio degli incidenti della Polizia Municipale.

23. COLLEGAMENTO DA REMOTO FORNITORI ESTERNI

1. Il collegamento da remoto da parte di fornitori dell'Ente avviene tramite firewall di rete con lo stesso procedimento visto per il telelavoro oppure attraverso un programma evoluto di accesso remoto simile a quello citato nell'art. 10.
2. Tutte le connessioni avvengono in modalità sicura e le ditte possono solo operare previo consenso dell'Ufficio coordinamento e sviluppo informatico o in subordine dell'utente coinvolto nella chiamata di assistenza.
3. Per policy di dominio della rete informatica comunale gli accessi ai server sono permessi sempre per mezzo di personale dell'Ufficio coordinamento e sviluppo informatico che monitora e cura tutte le fasi del collegamento.

24. PAGOPA

1. L'Ufficio coordinamento e sviluppo informatico seguendo le linee guida di AGID ha attivato il servizio di pagamenti tramite PagoPa
2. Tutti i pagamenti on line presenti sul sito internet istituzionale sono stati dismessi e verranno ripristinati attraverso la tecnologia di PagoPa
3. I servizi di pagamento sono in modalità 1 con servizi di pagamento spontaneo.

25. APP E SOCIAL

1. Oltre al canale istituzionale del sito web, il Comune di Novi Ligure gestisce una applicazione per cellulari e tablet denominata App Municipium.
2. L'app fa parte di una rete di comuni aderenti al progetto e gestisce le aree tematiche quali la gestione degli eventi, delle notizie, della protezione civile e delle informazioni utili.
3. Oltre a gestire in maniera indipendente le informazioni, la app è configurata per riportare le notizie del sito internet comunale.
4. L'ufficio coordinamento e sviluppo informatico, di concerto con l'ufficio stampa e l'urp, gestisce le informazioni del sito internet comunale e divulga notizie anche sul canale twitter, sul canale youtube e su facebook.

26. VOIP

1. Il Comune di Novi Ligure ha due sedi principali collegate in fibra ottica. La struttura comunale comprende poi le sedi della polizia municipale, della biblioteca civica, magazzino comunale, museo dei campionissimi, cimitero, asilo aquilone, asilo girasole e mensa comunale
2. Come specificato nell'articolo 7 comma 2 il centro stella della rete informatica comunale è situato presso l'Ufficio coordinamento e sviluppo informatico dove sono situati i centralini voip comunali.
3. Il voip è attivo presso le due sedi principali presso la polizia municipale e presso la biblioteca civica.
4. Nei computer comunali, per 40 utenze, è presente un software di gestione della fonia che permette la visione e la gestione delle telefonate.

27. LAVORO AGILE E TELELAVORO – EMERGENZA COVID-19

1. VISTO il DCPM dell'8 marzo 2020 "Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19" all'art. 2 comma r) la modalità di lavoro agile disciplinata dagli articoli da 18 a 23 della legge 22 maggio 2017, n. 81, può essere applicata, per la durata dello stato di emergenza di cui alla deliberazione del Consiglio dei ministri 31 gennaio 2020, dai datori di lavoro a ogni rapporto di lavoro subordinato, nel rispetto dei principi dettati dalle menzionate disposizioni, anche in assenza degli accordi individuali ivi previsti; gli obblighi di informativa di cui all'art. 22 della legge 22 maggio 2017, n. 81, sono assolti in via telematica anche ricorrendo alla documentazione resa disponibile sul sito dell'Istituto nazionale assicurazione infortuni sul lavoro

2. L'ufficio coordinamento e sviluppo informatico aderendo alle disposizioni del DCPM di cui al comma 1 e dei successivi aggiornamenti e in ottemperanza alle misure minime di sicurezza ha predisposto l'acquisto e la messa in funzione di ulteriori portatili per l'accesso in tutta sicurezza tramite VPN coma da capitolo 20 "Telelavoro".
3. L'ufficio coordinamento e sviluppo informatico ha inoltre divulgato ai dipendenti esclusi dal telelavoro o dalle connessioni in vpn la possibilità di operare alla maggior parte dei servizi con il proprio apparecchio informatico con le seguenti modalità:

- il servizio di posta elettronica è escluso all'accesso del dominio comunale se non attraverso l'inoltro della posta al proprio personale (ma la risposta avverrebbe tramite posta personale) o tramite l'accesso con CAL del programma di posta elettronica Microsoft Exchange (richiesta da fare all'ufficio coordinamento e sviluppo informatico)
- il file server del comune contenente i documenti slegati dalle procedure è inaccessibile se non per una quantità minima attivata in cloud dietro richiesta all'ufficio coordinamento e sviluppo informatico
- le procedure aderenti alla ditta APkappa sono accessibili tramite server esterno mentre le rimanenti procedure essendo locali ne rimangono escluse.

4. Per tutti i dipendenti in telelavoro vpn inoltre esiste la possibilità di far accedere al proprio portatile da parte dell'ufficio coordinamento e sviluppo informatico tramite la seguente modalità:

- Si utilizza Chrome Remote Desktop che è una estensione (app) del browser chrome una volta installata con utente amministrativo del PC
- Dopo l'accesso, attraverso un account Google privato un utente può "Richiedere assistenza" e generare un codice
- Un altro utente Google remoto dalla stessa applicazione può "Dare assistenza" usando il codice che ha una validità temporale di pochi minuti e si connette al PC che ha chiesto assistenza.

5**. Video conferenze**: per quel che riguarda le video conferenze e la gestione condivisa del desktop si ricorda che i pc all'interno della rete informatica comunale non sono provvisti di videocamera ed è necessario richiederne l'aggiunta per effettuare videochiamate. Per tutti gli utenti della rete informatica in telelavoro o in smart workig e per gli utenti esterni è possibile effettuare chiamate Skype. Si stanno attivando diversi canali quali Tim Work già utilizzata per conferenze capogruppo, G-suite e Wildix. Per Tim Work, già attiva, l'amministratore del canale virtuale apre una stanza virtuale e gli interlocutori per un massimo di 25 accedono alla stanza virtuale cliccando sul link tramite browser. Occorre quindi prenotare la stanza tramite richiesta all'ufficio coordinamento e sviluppo informatico. Per Wildix avremo la possibilità di gestire più amministratori per la creazione di stanze virtuali di videoconferenza.

28. DISPOSIZIONI FINALI

1. I responsabili di struttura (dirigenti e posizioni organizzative) vigilano, nei limiti delle norme legali e contrattuali, sul rispetto delle regole contenute nel presente regolamento.
2. In caso di violazione del regolamento e delle disposizioni legislative in materia di sicurezza informatica, il soggetto competente in materia di procedimento disciplinare curerà l'attivazione dell'istruttoria in sintonia con quanto stabilito nei casi e nei modi previsti dalla normativa vigente.

3. Per quanto non espresso nel presente regolamento si rinvia al Documento delle misure minime di sicurezza depositato presso l'Ufficio coordinamento e sviluppo informatico e allegato al presente