DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

Comune di
NOVENTA DI PIAVE
(Provincia Venezia)

04	05/05/2009	Quarta Emissione Mod par 13.4 - 13.3.3- 13.6.1 - Cap 15	➢ Maschietto Donatella ➢ Michele Scaramal	dr. Alessandro Rupil
03	26/02/2008	Terza Emissione Mod par 13.4 - 13.3.3- 13.6.1 - Cap 15	➢ Maschietto Donatella ➢ Michele Scaramal	dr. Alessandro Rupil
02	27/03/2007	Seconda Emissione	➢ Maschietto Donatella ➢ Michele Scaramal	dr. Alessandro Rupil
01	23/12/2005	Prima Emissione	➢ Maschietto Donatella ➢ Michele Scaramal	dr. Alessandro Rupil
Rev.	Data	Causale	Preparato da	Titolare Trattamento dei Dati

INDICE

1. PREMESSA

Il patrimonio informativo di ogni Amministrazione comunale rappresenta un bene di importanza fondamentale che deve essere salvaguardato garantendone l'integrità e la riservatezza. Oggi con l'avvento delle nuove tecnologie e la complessità dei sistemi informativi il tema della sicurezza informatica, assume sempre più una rilevanza strategica. Il problema non riguarda solamente gli enormi danni causati dai virus informatici o gli attacchi provenienti dall'esterno da parte di hacker, ma anche il comportamento degli utenti ed il corretto utilizzo delle apparecchiature e degli strumenti messi a disposizione dalla tecnologia informatica. Una corretta politica di gestione della sicurezza è in grado di limitare i danni dovuti al diffondersi di informazioni riservate o a violazioni dell'integrità delle informazioni. Oltre a questi aspetti la normativa vigente in termini di privacy impone anche alle Amministrazioni che trattano dati sensibili di attuare una serie di misure minime per la sicurezza dei dati.

Il presente documento è stato redatto e viene tenuto aggiornato, ai sensi e per gli effetti dell'art. 31 del Decreto Legislativo 30 giugno 2003, n. 196, e tenuto conto del punto 19 dell'Allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza", dal Comune di NOVENTA DI PIAVE (di seguito, per brevità, il "Titolare"). Il documento è custodito presso **l'ufficio della Segreteria** e riporta, in sintesi, i risultati emersi dalla valutazione e dalle misure attuate e da effettuarsi per il rispetto della normativa in materia di protezione dei dati personali vigente alla data di redazione e aggiornamento del presente documento.

Nella redazione e aggiornamento del presente documento il Titolare è ricorso ai seguenti criteri: congruità dimensionale, congruità numerica degli addetti, congruità della strumentazione tecnologica.

L'attività del Titolare è esercitata perseguendo e ispirandosi alle attività oggetto della propria impresa.

Nelle intenzioni del Titolare risulta, quindi, fondamentale un sistema di protezione per la sicurezza dei dati personali adeguato sia al tipo, alle finalità, all'ambito, agli strumenti del trattamento dei dati stessi, sia allo stato della tecnologia. A tal fine, il presente documento vuole, oltre che adempiere agli obblighi legislativi, rappresentare il manuale organizzativo della pianificazione della sicurezza dei dati personali, contenente per ciò le istruzioni, le direttive e le linee guida destinate ai soggetti che prestano, a vario titolo (dipendenti, consulenti, collaboratori, etc.), la propria opera in favore del Titolare, entrando in contatto (fisico o elettronico) con i dati da quest'ultimo trattati.

L'attività del Titolare è esercitata nel rispetto degli scopi previsti dallo statuto e dalle leggi vigenti. Nell'ambito dello svolgimento di tale attività, il Titolare attribuisce valore ai dati e alle informazioni di cui dispone, tanto da considerarli patrimonio da salvaguardare e proteggere. Tra questi sono di particolare importanza i dati personali, intesi come qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Il Titolare è, altresì, consapevole del fatto che il trattamento dei dati personali è ricompreso dall'art. 15 del d. lgs. n. 196/03 (di seguito, per brevità, il "Codice Privacy"), tra le attività pericolose disciplinate dall'art. 2050 del Codice Civile, ai sensi del quale "chiunque cagiona danno ad altri nell'esercizio di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno".
Consapevole di ciò, e compatibilmente con l'esercizio efficiente delle proprie attività, i dati vengono utilizzati dal sistema informatico di cui il Titolare si avvale solo quando le finalità perseguite non possono essere realizzate impiegando dati anonimi e/o statistici.

Tutto il personale dipendente, come anche i consulenti e collaboratori a vario titolo, sono stati adeguatamente informati e responsabilizzati sull'obbligo su di essi incombente di:
trattare i dati in modo lecito e secondo correttezza, per scopi determinati e legittimi, assicurandosi che i dati personali oggetto del trattamento siano esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti;
rispettare, nell'ambito del trattamento dei dati e delle informazioni, il principio della riservatezza.

Il generale principio della riservatezza è dal Titolare inteso, in relazione alle proprie attività, come:
divieto di comunicare i dati personali, anche in via incidentale, sia all'interno sia all'esterno, salvo i casi di esecuzione delle procedure dell'ente predefinite o previa verifica della legittimità del destinatario a ricevere le informazioni;
obbligo di provvedere alla conservazione e alla custodia degli stessi in modo da ridurre al minimo i rischi di:
distruzione o perdita (totale o anche solo parziale), anche accidentale;
accesso non autorizzato;
trattamento non consentito o non conforme alle finalità della raccolta.

obbligo di preservare l'integrità, la disponibilità agli utenti autorizzati e la conservazione degli stessi per il tempo necessario alle finalità per le quali sono stati raccolti, provvedendo poi alla relativa distruzione, salvo eventuali obblighi di archiviazione prescritti dalle procedure predefinite.
E ciò, non solo per adempiere agli obblighi imposti dalla legge e in particolare dal Codice Privacy, ma per offrire agli associati quei requisiti di precisione, efficienza e soprattutto riservatezza che devono caratterizzare le attività del Titolare.

Pertanto, il personale dipendente, come i collaboratori e consulenti a vario titolo, dovrà informare gli interessati sulle modalità relative ai trattamenti, consegnando loro gli appositi moduli di informativa e raccogliere i consensi richiesti, documentando la ricezione secondo la procedura adottata dal Titolare descritta dal presente documento.

Per il Titolare risulta quindi fondamentale un adeguato sistema di protezione per la sicurezza dei dati; a questo fine il presente documento vuole, oltre che adempiere agli obblighi legislativi, dare un'ulteriore impronta di affidabilità del Titolare stesso.

2. SCOPO

Il Documento Programmatico sulla Sicurezza definisce le norme, e le direttive e le misure tecniche, organizzative e procedurali che sono adottate dal Comune di NOVENTA DI PIAVE per la salvaguardia delle informazioni e dei dati trattati dal Titolare svolte sia con l'ausilio di strumenti elettronici sia senza l'ausilio degli stessi. Il presente documento intende fornire inoltre le indicazioni, direttive e istruzioni sulle modalità di applicazione del Codice Privacy alle risorse del Titolare, e più in generale su tutto quanto riguarda il corretto trattamento dei dati.

3. CAMPO DI APPLICAZIONE

Il presente piano Programmatico sulla Sicurezza, previsto dalla norma attuativa (D.L. 196/2003), si applica a tutti i dati trattati all'interno dal Titolare o, per incarico dello stesso, gestiti all'esterno presso terzi, sia con strumenti elettronici o comunque automatizzati che con altri strumenti e supporti, anche non elettronici.
Esso è l'atto conclusivo di una serie complessa di verifiche sullo stato della "sicurezza informatica" nel comune. L'adeguamento alla normativa, che prevede un aggiornamento dello stesso documento entro il 31 marzo di ogni anno, sarà un'occasione per effettuare una valutazione complessiva sul Sistema Informatico Comunale nel suo complesso ed eventualmente programmare miglioramenti sia in termini di sicurezza.
La presente procedura si applica alle sedi sotto identificate:

Denominazione	Ubicazione
Sede Municipale	Piazza G. Marconi 1
Biblioteca Comunale	Via Giacomo Noventa 19
Archivio storico	Via Torino 18

Questo documento stabilisce anche i compiti e le responsabilità dei soggetti che, a vario titolo e con diverse funzioni e responsabilità, sono coinvolti nel trattamento dei dati e i soggetti da questi delegati.

4. CONCETTI, ABBREVIAZIONI, DEFINIZIONI

SW: software

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

Dati Personali: qualunque informazione relativa a persona fisica,persona giuridica,ente od associazione, identificati o identificabili , anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dati identificativi: i dati personali che permettono l'identificazione diretta del interessato;

Dati sensibili: dati idonei a rivelare l'origine razziale etnica, le convinzioni religiose, filosofiche o di altro

genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati Giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1, lettere da a) a o) e da r) a u) del DPR 14 novembre 2002, n 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile: La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente preposti dal titolare al trattamento dei dati personali

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Interessato: persona fisica, persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Amministratore di sistema: i soggetti cui è conferito il compito di sovrintendere alle risorse dei sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Rischio: con il termine di rischio si identifica l'esposizione alla possibilità di ottenere un guadagno o una perdita economica o finanziaria, di sopportare un danno fisico o un ritardo, come conseguenza dell'incertezza associata al perseguimento di un determinato corso d'azione

5. NORMATIVA DI RIFERIMENTO

Le norme a cui si fa riferimento:

la Carta dei Diritti Fondamentali dell'Unione Europea e in particolare l'art. 8;
la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995;
il Codice in materia di Protezione dei Dati Personali (decreto legislativo 30 giugno 2003, n. 196).

6. COMPITI E RESPONSABILITÀ

Le figure identificate dalle disposizioni vigenti in materia di trattamento dei dati sono:

Titolare:

- ha potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile Sistemi Informativi:

- ha il compito di verificare che la policy venga applicata correttamente nell'ambito delle proprie competenze;
- ha il compito di garantire che il DPS venga aggiornato entro il 31 marzo di ogni anno;
- ha il compito di promuovere e proporre soluzioni che migliorano la sicurezza del sistema informativo del Comune.
- ha il compito di indire periodicamente un incontro per valutare le attività e le proposte dei vari responsabili in materia di sicurezza.

Responsabile trattamento dei dati:

- ha il compito di attuare le politiche di sicurezza nell'ambito del settore di competenza.
- si incarica di suggerire e promuovere azioni che migliorino la sicurezza dei dati trattati dall'ente.

Amministratore di sistema:

- ha il compito di gestire e sovraintendere al buon funzionamento del sistema informativo.
- deve proporre e promuovere iniziative e soluzioni tecnologiche ed organizzative per migliorare l'efficienza e la sicurezza del sistema informativo.
- deve attuare le misure di sicurezza informatiche definite nel DPS

- attua le regole di autenticazione informatica conformemente al D Lgs 196/03
- configura gli apparati e gli applicativi di sicurezza in modo da garantire un'efficace protezione del sistema informativo del Comune.
- imposta in modo corretto le regole di backup degli archivi informatici.
- installa e configura i sistemi operativi dei server, dei personale computer.
- installa e configura gli apparati di rete e di sicurezza perimetrale

Custode delle Password:

- il soggetto o i soggetti preposti alla custodia delle parole chiave o che hanno accesso ad informazioni che concernono le medesime.
- le password verranno custodite in una busta chiusa custodito in un cassetto chiuso a chiave.

Sanzioni:
il presente documento pone quindi una serie di istruzioni, direttive e linee guida poste a salvaguardia dei dati degli interessati e del Titolare, costituenti tutti e ciascuna di essi dati patrimonio del Titolare stesso. Pertanto, l'eventuale inosservanza o violazione di tali istruzioni, direttive e linee guida costituisce infrazione disciplinare, ai sensi e per gli effetti dell'art. 7 della Legge n. 300/70 (cosiddetto Statuto dei Lavoratori) e del vigente ed applicabile contratto collettivo nazionale e individuale di lavoro, nonché grave inadempimento ai sensi e per gli effetti dell'art. 1453 del Codice Civile, suscettibile di produrre le conseguenze previste dalla legge, nonché dal contratto collettivo nazionale e individuale di lavoro.

Nell'ambito del Comune di NOVENTA DI PIAVE vengono identificate le seguenti figure:

Incarico	P.O. / U.O.	Responsabile
Titolare	Segretario Comunale	dr. Alessandro Rupil
Responsabile trattamento dei Dati	P.O. Affari Generali	Donatella Maschietto
Responsabile trattamento dei Dati	P.O. Economico Finanziaria	rag. Ivo Biancotto
Responsabile trattamento dei Dati	P.O. Servizi Tecnici	arch. Nicoletta Modanese
Responsabile trattamento dei Dati	P.O. Polizia Locale	Francesco Paolo Guerra
Amministratore del sistema Informativo	U.O. Informatica	Michele Scaramal
Amministratore Password	U.O. Informatica	Michele Scaramal

Per completezza, si è ritenuto utile e opportuno allegare al DPS una serie di documenti che rendono, con immediatezza, intelligibile a quanti sono coinvolti, a vario titolo, nella politica di protezione e sicurezza dei dati personali adottata dal Titolare, nonché agli organi ispettivi, la politica di protezione e sicurezza dei dati personali (security and data protection policy).

7. DOCUMENTI ALLEGATI

- Analisi dei rischi

8. COMPOSIZIONE DEL DOCUMENTO

Il DPS prevede una prima fase chiamata "Identificazione delle Risorse da Proteggere"; risorse che, in diverso modo, operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati.

A tal proposito, una volta individuati i dati da proteggere, tramite un'altra fase, definita di Analisi dei Rischi, sono state valutate e studiate le minacce e le vulnerabilità a cui tali risorse (i dati per l'appunto) sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità e la conservazione di ogni singolo dato personale trattato.

Dall'analisi dei rischi si è redatto un Piano di Sicurezza, tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Inoltre è stato definito un Piano di Verifiche delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari.

9. REVISIONE DEI DOCUMENTI

L'emissione e la revisione della Documento Programmatico della Sicurezza, avviene nel rispetto di regole precise e sotto la sorveglianza del Responsabile del Servizio Informativo che garantisce uno sviluppo equilibrato e congruente con l'evoluzione del sistema informativo del Comune.

Il documento viene redatto, aggiornato e tenuto ai sensi dell'art. 34, comma 1, lett. g), d. lgs. 30 giugno 2004, n. 196 e del punto 19 dell'Allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza"

Le regole da seguire per i vari tipi di documenti sono le seguenti:

Il DPS contiene le politiche di sicurezza del Comune. Eventuali modifiche della policy e revisioni del documento possono essere suggerite per iscritto da qualsiasi collaboratore dell'ente al Responsabile del Servizio Informativo che le valuta e decide per un'eventuale modifica.

L'analisi dei rischi identifica i possibili eventi indesiderati che possono causare un danno alle risorse del sistema informativo. Una revisione del documento può essere determinata da una serie di motivi, variazione dell'impianto informativo, mutate condizioni organizzative o logistiche.

Le modifiche accolte dall'Amministratore del Sistema Informativo portano alla revisione del Documento Programmatico della Sicurezza o della Risk Analysis. Va ribadito che l'iter di controllo e approvazione dei documenti, di cui ai punti precedenti, deve rispecchiare quello della prima emissione, a meno di cambiamenti del personale dell'ente o di cambiamenti organizzativi. Per ogni modifica effettuata si aggiorna progressivamente il numero della revisione.
La focalizzazione delle modifiche introdotte con le varie revisioni viene effettuata mediante un segno di evidenziazione del testo. Nel caso di revisione generale, i contenuti della procedura variati sono tali da considerarne una nuova impostazione.
L'aggiornamento dell'archivio cartaceo e di quello elettronico, relativi al DPS, è compito dell'Amministratore del Sistema Informativo.
Quando un Documento della sicurezza è revisionato, l'Amministratore del Sistema Informativo, conserva la copia superata in formato elettronico in un apposita directory denominata "Doc_Sicurezza_Superati".

Documento	Redazione	Approvazione	Distribuzione	Archiviazione
DPS	➢ P.O. Affari Generali ➢ Responsabile Sistema Informativo	Titolare	➢ P.O. Affari Generali ➢ Responsabile Sistema Informativo	➢ P.O. Affari Generali ➢ Responsabile Sistema Informativo
Analisi dei rischi	➢ P.O. Affari Generali ➢ Responsabile Sistema Informativo	Titolare	➢ P.O. Affari Generali ➢ Responsabile Sistema Informativo	➢ P.O. Affari Generali ➢ Responsabile Sistema Informativo

10. IDENTIFICAZIONE DELLE RISORSE

Le risorse che in qualche modo intervengono nel trattamento dei dati del titolare sono identificate da:

- Luoghi fisici
- Apparecchiature
- Banche dati
- Personale

Di seguito verrà data una descrizione sommaria di questi elementi.

10.1. Luoghi Fisici

i luoghi fisici dove si svolge il trattamento dei dati sono identificati nel paragrafo capitolo 6

10.2. Sistema Informativo

10.2.1. Server

Il sistema informativo del comune di NOVENTA DI PIAVE si compone di una serie di server installati all'interno di un locale accessibile al personale dell'ufficio informatico tramite serratura.
Sui server sono installate le banche dati del comune e l'accesso alle banche dati avviene tramite Rete Locale.
Nella tabella sotto riportata sono identificati i server, il sistema operativo installato e il data base

Nome Server	Sistema Operativo	Banca Dati	Caratteristiche Hw
NoventaServer	Windows 2003 server	➢ Sicra ➢ DB MSsql ➢ Cartelle condivise	DL 380 G5 CPU xeon 3,2 ghz Ram 4 Gb HD n°3 72 GB RAID 5
NoventaBiblo	Windows 2000 server sp4	➢ Bibliotaca	PIII 1 GB RAM 4x4,3Gb RAID 5 SCSI
Storage dati	HP Ultrium 232	➢ Banche dati del comune	Capacità 200 GB

10.2.2. Networking

Gli apparati attivi di rete sono identificati di seguito

Descrizione	Marca	Modello	Ubicazione
Firewall	CISCO	PIX 506E	Sala CED
Router ADSL Internet	Digicom	Digicom	Sala CED
3 Switch	HP	HP 2524	Sala CED
Router ISDN Internet (scorta)	ZYXEL	PRESTIGE 400	Sala CED
Firewall e Proxy Biblioteca	Piattaforma Linux	Firewall, proxy, Content Filtering, ids	Biblioteca
Router ADSL	Allied Telesis	FXV 2409 LEV	Biblioteca
Switch	Level One		Biblioteca

Questi apparati sono custoditi in un armadio chiuso a chiave all'interno della sala server.
Il servizio di collegamento alla rete pubblica è gestito da un provider tramite un collegamento ADSL. Oltre a questo servizio, presso il comune è installato un modem utilizzato per la teleassistenza.

La rete LAN è una rete basata su sistema operativo Microsoft e dominio di windows 2000.

10.2.3. Personal Computer

I PC in dotazione ai collaboratori del comune sono dotati di sistemi operativi windows. Le macchine sono censite dal responsabile dei sistemi informativi, che ha creato delle schede con la configurazione di ogni PC. Su ogni di essi è installato l'antivirus che viene periodicamente aggiornato.
L'accesso alla risorse di rete avviene tramite account composto da un identificativo e da una password.

10.2.4. Risorse Software

Sono di seguito elencate gli applicativi software utilizzati per il trattamento dei dati

Servizio	Nome del software	Fornitore
Protocollo e albo	Sicra-Lotus Notes	SAGA SPA
Delibere e Determine	Sicra-Lotus Notes	SAGA SPA
Bilancio	Sicra	SAGA SPA
Economato ed inventario	Sicra	SAGA SPA
Tributi	Sicra	SAGA SPA
Codici fiscali	Siatel	Ministero delle Finanze
Servizi Demografici	Sicra	SAGA SPA
Cittadini residenti all'estero	Anag Aire	Ministero Interni
Anagrafe e stato civile	Sicra	SAGA SPA
Servizi sociali	File Office	Microsoft
Rilevazione presenze	Time2 Win	SAGA SPA
Gestione Vigilanza	Polcity	SAGA SPA
Gestione Ufficio Tecnico	CnedWeb	Datapiano srl
Ufficio Tecnico - Programmazione Triennale	Programma Triennale	CEL srl

Posta elettronica	Lotus Notes	SAGA SPA
Biblioteca	SOSEBI TLM	SoSeBi

10.3. Classificazione dei Dati e delle Informazioni

I dati gestiti dall'agenzia informatica del comune di NOVENTA DI PIAVE sono stati classificati in tre tipologie:

- Dati Sensibili
- Dati Giudiziari
- Dati Personali

Gli archivi cartaceo ed elettronici gestiti dal Comune sono di seguito identificati:

TABELLA CLASSIFICAZIONE DELLE BANCHE DATI									
P.O.	**Ufficio Incaricato**	**Tipologia di dati trattati**	**Mod Trat**	**Tip. Trat**	**Nat. Trat**	**Data Base**	**Server di memorizzazione**	**Fornitore**	**Modalità di connessione**
Tutte	Tutti	Anagrafica persone fisiche e giuridiche del comune.	E	B	P	Sicra – DB SQL	NoventaServer	SAGA SPA	LAN
Tutte	Tutti	Delibere Consiglio Comunale Delibere Giunta Comunale	E/D	A	P/S/G	Lotus Notes	NoventaSicra	Saga SpA	LAN
Tutte	Tutti	Determinazioni	E/D	A	P/S/G	Lotus Notes	NoventaSicra	Saga SpA	LAN
Tutte	Tutti	Protocollazione corrispondenza in uscita	E/D	A	P/S/G	Lotus Notes	NoventaSicra	Saga SpA	LAN
Tutti	Tutti	Archivio Posta Elettronica	E	A	P/S	Lotus Notes	NoventaSicra	SAGA SPA	LAN
Affari Generali	Segreteria/Protocollo	Corrispondenza degli assessori	E/D	A	P	File Office	NoventaSicra	---	LAN
Affari Generali	Segreteria/Protocollo	Verbali di riunioni degli amministratori e delle commissioni	E/D	A	P	File Office	NoventaSicra	---	LAN
Affari Generali	Segreteria/Protocollo	Contratti affidamento lavori, servizi di concessione	E/D	A	P	File Office	NoventaSicra	---	LAN
Affari Generali	Segreteria/Protocollo	Dati relativi agli incarichi professionali, repertorio dei contratti	E/D	A	P	File Office	NoventaSicra	---	LAN
Affari Generali	Segreteria/Protocollo	Concessioni Cimiteriali	E/D	A	P	File Office	NoventaSicra	SAGA SPA	LAN
Affari Generali	Segreteria/Protocollo	Banca dati degli amministratori comunali	E/D	A	P	File Office	NoventaSicra	---	LAN
Affari Generali	Segreteria/Protocollo	Banca dati relativa alle associazioni a cui il comune aderisce	E/D	A	P	File Office	NoventaSicra	---	LAN
Affari Generali	Segreteria/Protocollo	Banca dati relativa al fondo del culto.	E/D	A	P	File Office	NoventaSicra	---	LAN
Affari Generali	Segreteria/Protocollo	Archivio storico del comune contenente i dati relativi alla gestione dell'ente	D	A	P/S/G	---	---	---	---
Affari Generali	Segreteria/Protocollo	Protocollazione della corrispondenza in entrata ed in uscita.	E/D	A	P/S/G	Lotus Notes	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Sociali	Cartelle utenti servizi Anziani Disabili, tutela minori, servizi minori	E/D	A	P/S	File Office	NoventaSicra	---	Locale
Affari Generali	Servizi Sociali	Cartelle utenti servizi tutela	E/D	A	P/S	File Office	NoventaSicra	--	Locale
Affari Generali	Servizi Sociali	Cartelle utenti servizi minori	E/D	A	P/S	File Office	NoventaSicra	--	LAN
Affari Generali	Servizi Sociali	Dati relativi ai servizi erogati dal comune e dei cittadini che ne usufruiscono	E/D	A	P/S	File Office	NoventaSicra	---	LAN

Affari Generali	Servizi Sociali	Dati relativi ai beneficiari dei contributi per buoni libro e borse di studio che comprendono essenzialmente dati anagrafici, dati relativi alle condizioni economico, famigliari.	E/D	A	P/S	File Office	NoventaSicra	---	LAN
Affari Generali	Servizi Sociali	Dati relativi ai beneficiari dei contributi di affitto che comprendono essenzialmente dati anagrafici, dati relativi alle condizioni economico, famigliari.	E/D	A	P/S	File Office	NoventaSicra	---	LAN
Affari Generali	Cultura/Pubblica Istruzione	Elenchi iscritti servizi scolastici (dato storico)	E/D	A	P/S	File Office	NoventaSicra	---	LAN
Affari Generali	Cultura/Pubblica Istruzione	Anagrafiche e contributi ad associazioni sportive e culturali	E/D	A	P/S	File Office	NoventaSicra	---	LAN
Affari Generali	Cultura/Pubblica Istruzione	Archivio della biblioteca del comune contenente l'anagrafica degli utenti e la movimentazione relativa ai prestiti.	E	A	P	BIBLO	NoventaBiblo	Provincia di Venezia	LAN
Affari Generali	Servizi Demografici	Dati relativi alla leva dei cittadini del comune, Ruoli Matricolari	E	A	P/G	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Dati relativi all'Anagrafe e all'AIRE dei cittadini del comune	E	A	P	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Dati relativi all'Anagrafe e all'AIRE dei cittadini del comune	E	A	P	AnagAire	NoventaSicra	Ministero degli Interni	Internet
Affari Generali	Servizi Demografici	Dichiarazioni e Permessi di soggiorno cittadini stranieri	E	A	P/S	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Giudici Popolari	E	A	P/S	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Dati relativi allo stato civile dei cittadini	E	A	P/S	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Albo Scrutatori, presidenti di seggio	E	A	P/S/G	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Fascicoli Elettorali	E	A	P/S/G	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Liste e tessere elettorali	E	A	P/S/G	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Dati relativi al personale eleggibile e ai cittadini che possono Votare	E	A	P/S/G	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Affari Generali	Servizi Demografici	Elenco carte di identità	E/D	A	P	Sicra – DB SQL	NoventaSicra	SAGA SPA	LAN
Economico Finanziaria	Personale	Fascicoli del personale	D	A	P/S	Archivio documentale		---	
Economico Finanziaria	Personale	Dati relativi alla gestione giuridica ed economica del personale dell'ente	E/D	A	P/S/G	File Office	*NoventaSicra*	---	LAN

Economico Finanziaria	Personale	Dati relativi alle presenze dei collaboratori dell'ente	E/D	A	P	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Personale	Dati relativi alle denunce mensili imponibili e Inadel	E	A	P	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Personale	Dati relativi agli infortuni sul lavoro o permessi per ferie o malattia	E	A	P	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Personale	Dati relativi alla gestione dei concorsi	E	A	P	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Personale	Dati relativi alle denunce fiscali e previdenziali	E	A	P	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Personale	Dati relativa al conto annuale del personale	E	A	P	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Personale	Gestione permessi sindacali e funzioni Pubbliche	E	A	P/S W	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Personale	Cartolarizzazione dei Crediti	E/D	B	P/S	Portale Inpdap	---	Inpdap	WEB
Economico Finanziaria	Personale	Denunce Infortuni	D	C	P/S	Archivio Documentale	---	---	LAN
Economico Finanziaria	Personale	Anagrafe delle Prestazioni	E	A	P	Portale Funzione Pubblica	---	Ministero Funzione Pubblica	LAN
Economico Finanziaria	Personale	Denunce DM10	E	A	P	INPS2000	*NoventaSicra*	INPS	FPT
Economico Finanziaria	Personale	Banca dati degli amministratori comunali	E	A	P	File Office	*NoventaSicra*	---	LAN
Economico Finanziaria	Ragioneria	Dati relativi alle entrate del comune, elenco creditori, elenco fornitori e professionisti	E/D	A	P	Sicra – DB SQL	NoventaSicra	*SAGA SPA*	LAN
Economico Finanziaria	Ragioneria	Dati contabili relativi agli amministratori, incarichi professionali, enti ed associazioni.	E/D	A	P	Sicra – DB SQL	NoventaSicra	*SAGA SPA*	LAN
Economico Finanziaria	Ragioneria	Mandati di Pagamento	E/D	A	P	Sicra – DB SQL	NoventaSicra	*SAGA SPA*	LAN
Economico Finanziaria	Ragioneria	Dati contabili relativi ai Fornitori	E/D	A	P	Sicra – DB SQL	NoventaSicra	*SAGA SPA*	LAN
Economico Finanziaria	Ragioneria	Banca dati degli amministratori comunali	E/D	A	P	File Office	NoventaSicra	---	LAN
Economico Finanziaria	Tributi	Dichiarazione e versamenti ICI	E/D	A	P	Sicra – DB SQL	NoventaSicra	*SAGA SPA Gest Line*	LAN
Economico Finanziaria	Tributi	Dichiarazione e versamenti ICIAP, TARSU, TOSAP.	E/D	A	P	Sicra – DB SQL	NoventaSicra	*SAGA SPA*	LAN

Economico Finanziaria	Tributi	Pubblicità e pubbliche affissioni	E/D	A	P	File Office	NoventaSicra	*Duomo GpA Serl*	LAN
Economico Finanziaria	Tributi	Codici Fiscali e posizioni tributarie	E	A	P	Siatel	----------	Ministero delle Finanze	Internet
Servizi Tecnici	AA.PP.	Dati relativi alle attività commerciali Intestatari Pubblici esercizi	D	A	P	File Office	NoventaSicra		LAN
Servizi Tecnici	AA.PP.	Banca dati polizia amministrativa, licenze e permessi sanitari	E/D	C	P/S	File Office	NoventaSicra	---	LAN
Servizi Tecnici	AA.PP.	Dati relativi alle attività delle agenzie d'affari rif art 163 D. Lgs 112/98	E/D	C	P/G	File Office	NoventaSicra	---	LAN
Servizi Tecnici	AA.PP.	Dati relativi ai certificati antimafia e Casellari Giudiziali attività commerciali	D	C	P/G	---	---	---	LAN
Servizi Tecnici	Ambiente	Dati relativi all'ambiente, attività della discarica, attività estrattive,	E/D	A	P/G	File Office	NoventaSicra	---	LAN
Servizi Tecnici	Ambiente	Convenzioni gestione rifiuti speciali	E/D	A	P/G	File Office	NoventaSicra	---	LAN
Servizi Tecnici	LL.PP.	Dati relativi alle gare d'appalto, ai progetti tecnici per la manutenzione del territorio e dei servizi di viabilità, di arredo pubblico	E/D	A	P/G	File Office	NoventaSicra	----	LAN
Servizi Tecnici	LL.PP.	Contratti affidamento lavori e servizi di concessione	D	B	P/G				
Servizi Tecnici	LL.PP.	Concessioni Cimiteriali	D	B	P/G				
Servizi Tecnici	LL.PP.	Dati relativi al patrimonio	E/D	B	P/G		NoventaSicra		LAN
Servizi Tecnici	LL.PP.	Autorizzazione scavi ad enti od aziende private	E/D	B	P/G		NoventaSicra		LAN
Servizi Tecnici	LL.PP.	Dati relativi alle imprese, ed ai professionisti che partecipano alle gare di appalto	E/D	B	P/G	File Office	NoventaSicra	----	LAN
Servizi Tecnici	LL.PP.	Casellari Giudiziari delle imprese che si aggiudicano un appalto di Lavoro	E/D	B	P/G		NoventaSicra		LAN
Servizi Tecnici	LL.PP.	Osservatorio dei Lavori Pubblici	E/D	B	P/G		NoventaSicra		LAN
Servizi Tecnici	Edilizia Privata	Banca dati relativa all'idoneità degli alloggi per carta di soggiorno	E/D	A	P	File Office	NoventaSicra	----------	LAN
Servizi Tecnici	Edilizia Privata	Banca dati relativa abitabilità	E/D	A	P	File Office	NoventaSicra	----------	LAN
Servizi Tecnici	Edilizia Privata	Dati relativi permessi di costruzione, Dia, condono edilizio	E/D	A	P	File Office	NoventaSicra	----------	LAN
Servizi	Edilizia Privata	Banca dati sportello unico per l'edilizia.	E/D	A	P	File Office	NoventaSicra	----------	LAN

Tecnici									
Servizi Tecnici	Edilizia Privata	Titolari Concessioni edilizie, DIA, Ordinanze, Anagrafe tributaria, Statistiche Istat	E/D	A	P	File Office	NoventaSicra	----------	LAN
Servizi Tecnici	Edilizia Privata	Cartografia	E/D	A	P	File Office	NoventaSicra	----------	LAN
Servizi Tecnici	Edilizia Privata	PRG, Piani Urbanistici attuativi	E/D	A	P	File Office	NoventaSicra	----------	LAN
Servizi Tecnici	Manutenzioni	Dati relativi alle ditte per forniture materiali e prestazioni di servizi	D	A	P			----------	LAN
Polizia Locale	Polizia Locale	Anagrafe canina	E/D	A	P/S	File Office	NoventaSicra	---	LAN
Polizia Locale	Polizia Locale	Registro cartaceo denuncia permessi per stranieri	E/D	C	P/S	File Office	NoventaSicra	---	LAN
Polizia Locale	Polizia Locale	Autorizzazioni temporanee pubblici esercizi	E/D	A	P	File Office	NoventaSicra		LAN
Polizia Locale	Polizia Locale	Autorizzazioni attività ricettive e spettacoli viaggianti	E/D	A	P	File Office	NoventaSicra		LAN
Polizia Locale	Polizia Locale	Ordinanze	E/D	A	P	Lotus Notes	NoventaSicra	SAGA SPA	LAN
Polizia Locale	Polizia Locale	Registro notificazioni	E/D	A	P	Lotus Notes	NoventaSicra	SAGA SPA	LAN
Polizia Locale	Polizia Locale	Dati relativi ai Passi Carrai Occupazione suolo Pubblico Autorizzazioni interventi su suolo pubblico	E/D	B	P/G		NoventaSicra		LAN
Polizia Locale	Polizia Locale	Dati relativi alle infrazioni del codice della strada, Rilevazioni incidenti, Accertamento concessioni, Deroghe ordinanze codice stradale	E/D	A	P/G	Polcity	NoventaSicra	SAGA SPA	LAN
Polizia Locale	Polizia Locale	Dati relativi agli infortuni	E/D	A	P/G	Polcity	NoventaSicra	SAGA SPA	LAN
Polizia Locale	Polizia Locale	Permessi circolazione e Sosta per diversamente abili	D	A	P/S	File Office	NoventaSicra	----------	LAN
Polizia Locale	Polizia Locale	Registro sequestri / Rimozioni/ Fermi	D	A	P/S/G	----------	----------	----------	LAN
Polizia Locale	Polizia Locale	Provvedimenti ingiuntivi e sanzioni amministrative	D	A	P/S/G	----------	----------	----------	LAN
Polizia Locale	Polizia Locale	Richieste della procura di indagini, Atti polizia giudiziari	D	A	P/S/G	----------	----------	----------	LAN
Polizia Locale	Polizia Locale	Dati relativi ai TSO, richieste della Procura di indagine	E/D	A	P/S/G	File Office	NoventaSicra	----------	LAN

Tutti	Tutti	Archivio Posta Elettronica	E	A	P/S	Lotus Notes	NoventaSicra	SAGA SPA	LAN

Modalità trattamento	**Tipo di trattamento**	**Natura dati Trattati**
D: Documentale	A: Lettura; scrittura, salvataggio	P: personali
E: Elettronico	B: Lettura, Scrittura	S: Sensibili
	C: Lettura	G: Giudiziari

11. ANALISI DEI RISCHI

L'analisi dei rischi è un insieme di tecniche volte ad identificare gli eventi negativi e la loro probabilità di accadimento.
La stessa è stata condotta utilizzando una check list di riferimento per identificare aree, apparecchiature, prodotti software, procedure di gestione delle informazioni che potrebbero essere coinvolti da eventi rischiosi, quali perdita dei dati, danneggiamento degli stessi, interruzione del servizio del sistema informativo. Lo scopo di questa analisi è quello di identificare successivamente le azioni da intraprendere per migliorare il livello di sicurezza nel trattamento delle informazioni attraverso la pianificazione di una serie di interventi e la definizione di una serie di regole da applicare nel trattamento dei dati (Politica della Sicurezza).

11.1. Risk Assessment

In allegato è stato riportata la Risk Analysis condotto presso la sede municipale e la biblioteca di NOVENTA DI PIAVE. Il documento è stato suddiviso in una serie di paragrafi che fanno riferimento ai diversi step in cui si è suddiviso il lavoro di audit.

12. PIANO DI SICUREZZA

Nell'ambito del Comune di Noventa di Piave sono adottati una serie di procedimenti organizzativi volti a migliorare la sicurezza del sistema informativo.
Innanzitutto sono state identificati i ruoli e le responsabilità delle figure professionali che nell'ambito dell'ente trattano dati.
Le figure professionali identificate sono state formalmente incaricate attraverso una delega scritta che identifica competenze e responsabilità relative alla gestione della sistema informativo e al trattamento dei dati.
Le strutture all'interno dell'organizzazione complessiva del Comune che si occupano del trattamento di dati personali, anche in relazione ai compiti loro assegnati, sono state individuate in base alla tipologia, all'entità, alla distribuzione e alla organizzazione delle attività svolte all'interno dell'ente:
a tale scopo ciascun dipendente e collaboratore è incaricato ed autorizzato al trattamento dei diversi tipi di dati; gli incarichi - così come la responsabilità per la conservazione dei dati vengono conferiti personalmente al momento dell'inserimento di una nuova figura all'interno della struttura dell'ente;
ciascun incaricato può operare, per il trattamento dei dati, esclusivamente all'interno delle mansioni assegnate e in riferimento alle informazioni ed alle Banche dati disponibili relative alla propria categoria di appartenenza;
i soggetti che trattano dati riferiti all'attività del Comune che, per qualifica attribuita od in relazione alla concreta attività svolta, non rivestono la figura di incaricati, sono stati opportunamente autorizzati al trattamento mediante specifica Nomina.

Per quanto riguarda il Consiglio Comunale e la Giunta; tali organi non hanno poteri diretti di gestione delle banche dati, né operano eseguendo trattamenti. Tuttavia, al fine di svolgere appieno il mandato loro conferito, il sindaco, gli assessori e i consiglieri possono consultare ogni documento, sia cartaceo che informatico, anche contenente dati sensibili;

Società e ditte che effettuano la manutenzione dei Personal computer, dei software e delle reti informatiche e/o elaborazione dati. Tali soggetti operano in base a specifica autorizzazione, recante nel dettaglio i compiti e i limiti nell'espletamento dell'attività di assistenza. In particolare queste Ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione o, semplicemente, di verifica del funzionamento di un programma o di una attrezzatura informatica. A tal fine è praticamente obbligatorio accedere alle banca dei dati presenti sui personal computer o all'interno dei programmi software, evidenziando una conoscenza di dati personali che di per sé non è collegata allo scopo per cui la Ditta effettua la propria attività. Ai sensi del punto 25 del Disciplinare Tecnico allegato al D. Lgs. 196/2003, se l'adozione delle misure minime di sicurezza viene affidata a soggetti esterni alla propria struttura, quali i fornitori di programmi software dedicati, il Titolare del trattamento riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare Tecnico

richiamato.

Nell'ambito del Comune di Noventa di Piave sono adottati una serie di procedimenti organizzativi volti a migliorare la sicurezza del sistema informativo.
Innanzitutto sono state identificati i ruoli e le responsabilità delle figure professionali che nell'ambito dell'ente hanno un ruolo di responsabile nel trattamento dei dati.
Le figure professionali identificate sono state formalmente incaricate attraverso una delega scritta che identifica competenze e responsabilità relative alla gestione della sistema informativo e al trattamento dei dati. In particolare sono stati identificati:

- Responsabili del trattamento dei dati
- Responsabile delle password
- Amministratore di sistema
- Incaricati del trattamento

Sono inoltre state identificate le aziende esterne o professionisti che nell'ambito dell'incarico loro assegnato dal Comune trattano i dati gestiti dall'ente. Per queste aziende è stato inviata una nomina quale responsabile del trattamento dei dati in relazione al loro incarico.

12.1.1. Audit della sicurezza

E' stato predisposto un piano di audit per verificare periodicamente almeno una volta all'anno l'efficacia delle misure adottate e per rivedere l'analisi dei rischi. Il dettaglio è riportato nel capitolo "13.2 Sicurezza Fisica" del presente documento.

12.1.2. Formazione

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato del trattamento dei dati, con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza dei trattamento dei dati.
Per ogni utente il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni della normativa, le necessità di formazione.
All'Amministratore del Sistema è affidato il compito di verificare periodicamente la necessità di formazione degli utenti della rete, con lo scopo di fornire informazioni su nuove procedure di sicurezza e nuove metodologie applicate, anche in seguito ad aggiornamenti tecnologici.

12.1.3. Gestione profili di autorizzazione

Il procedimento prevede la comunicazione, al responsabile dei Sistemi Informativi, delle variazioni delle mansioni o dell'organico del comune da parte dell'ufficio del personale o dei responsabili di settore nel caso di variazioni di competenze all'interno di ogni singolo dipartimento.
Il responsabile dei sistemi informativi dovrà aggiornare gli incarichi per il trattamento dei dati e dovrà inoltre modificare i diritti di accesso alle risorse del sistema informativo e ai dati trattati in modo elettronico.

12.1.4. Gestione e comunicazione dell'Informativa

Come previsto nell'articolo 13 del D. Lgs 196/2003 il comune di Noventa di Piave ha predisposto dei modelli di informativa rivolti alle diverse categorie di soggetti interessati:

- Cittadini / Enti
- Dipendenti del comune
- Fornitori

L'informativa è stata pubblicata, presso i vari uffici e gli sportelli a cui il pubblico accede abitualmente.
Per il settore dei servizi sociali, quando si attiva un procedimento che prevede il trattamento di dati relativi allo stato di salute, il documento di informativa viene consegnato al soggetto interessato ed una copia controfirmata viene archiviata nella pratica.
Per i cittadini , ifornitori o gli enti di cui il comune tratta i dati è previsto la pubblicazione dell'informativa sul sito WEB del comune.

12.2. Sicurezza Fisica

La politica della sicurezza identifica i comportamenti che regolano l'accesso fisico a luoghi in cui sono conservati o custoditi dati personali o sensibili. A tale proposito si può identificare una classificazione degli stessi in:

- Aree ad accesso non controllato
- Aree ad accesso controllato
- Aree ad accesso ristretto

Per ognuna di queste sono state definite delle modalità di gestione degli accessi e delle regole per quanto riguarda l'installazione delle apparecchiature.

12.2.1. Controllo degli accessi agli edifici

Le sedi del comune in cui viene effettuato il trattamento dei dati sono identificate all'Art. 3 del presente DPS. Nella tabella sottostante vengono identificati i sistemi di controllo degli accessi ai vari edifici. Il Comune ha inoltre attivato un servizio di vigilanza notturna con una società specializzata.

Denominazione Sede	Sistema Sicurezza	Antincendio	Accesso all'Edificio
Sede Municipale	Il comune ha attivato un servizio di vigilanza notturno con una ditta specializzata.	All'interno dell'edificio è attivo un sistema antincendio con estintori, che viene periodicamente mantenuto da una ditta specializzata. Esiste una rilevazione fumi	L'accesso all'edificio avviene tramite due porte. L'accesso agli uffici dell'anagrafe durante l'orario di sportello è presidiato dal personale del settore. Al termine dell'orario di lavoro le porte vengono chiuse. Le porte e finestre del primo piano sono protette da inferiate.
Biblioteca	Il comune ha attivato un servizio di vigilanza notturno con una ditta specializzata.	All'interno dell'edificio è attivo un sistema antincendio con estintori, che viene periodicamente mantenuto da una ditta specializzata.	L'accesso alla Biblioteca che si trova al primo piano dell'edificio delle scuole elementari avviene tramite porta. L'accesso alla biblioteca durante l'orario di apertura è presidiato dal personale del settore.
Archivio	Il comune ha attivato un servizio di vigilanza notturno con una ditta specializzata.	All'interno dell'edificio è attivo un sistema antincendio con estintori, che viene periodicamente mantenuto da una ditta specializzata.	L'accesso all'archivio è consentito al solo personale autorizzato

12.2.2. Aree ad accesso non controllato

Sono quelle aree in cui il pubblico può accedere senza alcuna identificazione o misura di sicurezza. Rientrano in questa categoria la sala del consiglio, la sala riunioni, l'auditorium.
In queste aree non devono essere installate apparecchiature informatiche contenenti banche dati; non devono essere presenti apparecchiature collegate alla rete del comune, se le stesse non sono presidiate da un operatore; eventuali prese di rete devono essere disattivate; non devono essere presenti archivi documentali non adeguatamente protetti.

12.2.3. Aree ad accesso controllato

Sono quelle aree in cui può accedere solamente il personale dipendente dell'ente, nel caso in cui acceda del personale esterno questo deve essere identificato in un apposito registro o accompagnato da un collaboratore del comune. In questa tipologia rientrano anche le aree accessibili al pubblico che durante l'orario di apertura devono essere presidiate dai collaboratori del Comune.
Queste aree/uffici al termine dell'orario di lavoro o di chiusura degli sportelli devono essere chiuse al

pubblico.
In queste aree possono essere installate apparecchiature informatiche collegate alla rete interna.
Le stazioni di lavoro devono rispettare una serie di misure minime di sicurezza:

- accesso alle risorse del Sistema Informatico attraverso password conosciuta unicamente dall'operatore;
- le sessioni di lavoro devono essere protette da screen saver una volta che l'utente si è autenticato;
- eventuali apparati di rete devono essere disposti in armadi chiusi.

Gli archivi contenenti banche dati su supporto cartaceo devono essere chiusi a chiave, nel caso siano ubicati nelle aree di permanenza del pubblico.

12.2.4. Aree ad accesso ristretto

Sono quelle aree in cui sono installate apparecchiature critiche quali server, apparati di rete. L'accesso a tali aree è consentito solamente al personale autorizzato e devono essere all'interno di edifici sotto la responsabilità dell'Amministrazione Comunale.
I locali devono rimanere chiusi e le chiavi custodite dalle persone autorizzate.
L'accesso del personale esterno è regolamentato dal Responsabile.
Le aree ad accesso ristretto identificate presso il Comune di NOVENTA DI PIAVE sono essenzialmente:

- la SALA SERVER
- l'Archivio di Deposito e Storico

12.2.4.1. Regole di accesso SALA SERVER

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi. Le misure riguardano la sala server del comune accessibile attraverso una porta dotata di serratura la cui chiave è in dotazione al responsabile dei sistemi informativi e all'elettricista del comune.
Un'ulteriore copia delle chiavi è custodita dal responsabile dell'Ufficio Tecnico nel caso si debba accedere alla sala per motivi di emergenza in orari in chiusura degli uffici.

12.2.4.2. Accesso da parte del personale esterno

Il persone non dipendente che deve accedere al comune per la manutenzione degli apparati, degli applicativi software o degli impianti, deve registrare l'attività svolta sul registro di controllo degli accessi, indicando le proprie generalità, data di ingresso, data di uscita.
Quando delle persone entrano nella Sala macchine il loro operato è supervisionato da un collaboratore dell'ufficio informatico, che si preoccupa anche di impartire indicazioni inerenti le regole di accesso ai locali.
Nella tabella sottostante sono identificate le misure di protezione fisica della sala server e della sala macchine ubicate nei vari edifici nelle quali sono presenti apparati critici del sistema informativo dell'ente.

Identificazione	Palazzo	Modalità Accesso	Impianto antincendio	Impianto Condizionamento	Impianto Elettrico
Sala Server	Municipio	Serratura con chiave	si	si	si
Ufficio Informatico	Municipio	Serratura con chiave	si	si	si

12.2.4.3. Regole di Accesso all'Archivio Comunale

L'archivio del comune si distingue in archivio corrente, ed archivio storico.
L'archivio corrente è identificato nelle scaffalature e negli armadi degli uffici del comune, per i quali verranno identificate delle regole di accesso opportune.
L'archivio storico contiene dati e documenti, ed è ubicato in un locale del comune a cui possono accedere solamente le persone autorizzate.
L'archivio è dotato di impianto a rilevazione di fumi, che viene periodicamente revisionato dalla ditta esterna.

12.2.5. Misure di sicurezza e facility dell'edificio

Di seguito vengono identificate le misure adottate per la gestione della sicurezza e per la prevenzione di eventi naturali dannosi.

12.2.5.1. Antincendio

Nell'edificio sono presenti estintori facilmente individuabili e mantenuti da una ditta specializzata secondo le disposizioni di legge vigenti.

12.2.5.2. Impianto elettrico
L'impianto rispetta la normativa vigente. Eventuali interventi vengono svolti da ditte specializzate.

12.2.5.3. Alimentazione Elettrica - UPS
Per la protezione da sbalzi o mancanza di energia elettrica, tutti i server e i PC sono collegati ad un sistema UPS. Il sistema consente di alimentare le macchine rilevate alla data per circa 20 minuti. Nel caso di installazione di nuove apparecchiature, il limite minimo da non superare è di dieci minuti e questo deve essere valutato dal responsabile dei sistemi informativi.

12.2.5.4. Numeri telefonici di emergenza
I numeri telefonici delle ditte che curano l'assistenza hardware e software sono riportati in un elenco appeso nel locale ove sono custoditi il server di rete.

12.3. Politica degli accessi al Sistema Informativo e ai Dati

In questo paragrafo vengono identificate le politiche per la gestione logica della sicurezza delle informazioni che interessano quindi l'accesso alle basi di dati attraverso gli apparati del sistema informativo.

12.3.1. Identificazione utenti
Ogni utente può accedere alla rete del sistema informativo attraverso un identificativo (userid) univoco e password. L'identificativo e la password sono personali in modo che non sia possibile accedere da due postazioni di lavoro con lo stesso identificativo.
L'assegnazione dei diritti di accesso alla rete informatica o alla base di dati viene fatta dal responsabile del sistema informativo previa richiesta fatta dal responsabile di P.O.

12.3.2. Password
La password è assegnata a ciascun utente in forma riservata. Allo stesso è consentito di variarla. La gestione della password prevede una serie di misure sotto riportate atte a rendere efficace l'utilizzo della stessa:

- lunghezza minima 8 caratteri;
- deve essere sostituita ogni 3 mesi;
- non deve essere simile alla precedente;
- non deve essere comunicata ai colleghi;
- non deve essere annotata su supporti accessibili o leggibili;
- non deve contenere termini facilmente riconducibili all'incaricato.

12.3.3. Autenticazione
Il sistema informativo prevede due livelli di autenticazione:

- **autenticazione per accesso alle risorse del sistema**. Il Comune di NOVENTA DI PIAVE, utilizza i servizi di autenticazione del sistema operativo windows che prevedono la definizione della lunghezza minima delle password a 8 caratteri e l'utilizzo di una complessità nella definizione del codice di autenticazione.
- **autenticazione applicativa.** Per quanto riguarda gli accessi agli applicativi di business, sono state fornite precise istruzioni ai collaboratori sulla necessità di variare la password secondo le regole sopra indicate. Inoltre, per quelle soluzioni la cui gestione viene fatta da enti esterni, si deve prevedere la comunicazione della stessa all'amministratore delle password come evidenziato nella tabella di seguito riportata.

Solo agli "Amministratori di sistema" è consentito l'utilizzo condiviso della user 'master' per le attività di manutenzione dei sistemi operativi questa deve essere periodicamente variata con le regole sopra indicate. Nel caso un azienda esterna debba accedere alle risorse della LAN il responsabile dei sistemi informativi dovrà autorizzarne l'accesso identificandosi come amministratore ed avendo l'accortezza di non rivelare le credenziali di autenticazione.

Servizio/Applicativo	Nome del software	Gestione delle Password	Comunicazione delle password al responsabile
Amministrazione di rete	Windows2003	8 caratteri Scadenza 3 mesi	Si
Accesso alla rete	Windows2003	8 caratteri Scadenza 3 mesi	no
Protocollo e Albo	Lotus Notes	8 caratteri Scadenza 3 mesi	no
Delibere e Determine	Lotus Notes	8 caratteri Scadenza 3 mesi	no
Ragioneria	Sicra	8 caratteri Scadenza 3 mesi	no
Siatel	Siatel	8 caratteri Scadenza 3 mesi	si
Economato ed inventario	Sicra	8 caratteri Scadenza 3 mesi	no
Tributi	Sicra	8 caratteri Scadenza 3 mesi	no
Servizi Demografici	Sicra	8 caratteri Scadenza 3 mesi	no
ANAG AIRE	ANAG AIRE	8 caratteri Scadenza 3 mesi	si
Rilevazione presenze	Time2win	8 caratteri Scadenza 3 mesi	no
Polizia Locale	VisualPolcity	8 caratteri Scadenza 3 mesi	no
Ufficio Tecnico	CNEDWEB	8 caratteri Scadenza 3 mesi	no
Ufficio Tecnico	GIS	8 caratteri Scadenza 3 mesi	no
Posta elettronica	Lotus Notes	8 caratteri Scadenza 3 mesi	No
Assistente Sociale	File Office criptati	8 caratteri Scadenza 3 mesi	si
Biblioteca	TLM SoSeBi	8 caratteri Scadenza 6 mesi	si

12.3.4. Revoca delle password e dei permessi di accesso

La gestione dell'assegnazione dei diritti di accesso viene fatta responsabile del sistema informativo. Nel caso un collaboratore del comune si dimetta i diritti di accesso devono essere revocati attraverso una comunicazione all'amministratore del sistema da parte dell'ufficio del personale del Comune di NOVENTA DI PIAVE. Id e password utilizzate non possono essere associate ad un altro utente.

Nel caso in cui il collaboratore ricopra un incarico diverso deve essere fatta una comunicazione al responsabile del sistema informativo il quale provvede a modificare i permessi di accesso alle banche dati e alle risorse del sistema informativo.
La richiesta, deve essere fatta in forma scritta al Responsabile del Sistema Informativo da parte del Responsabile dell'Ufficio cedente e deve essere fatta una richiesta di attivazione da parte del Responsabile dell'Ufficio ricevente.
Le user-id inutilizzate per più di 6 mesi saranno disattivate autonomamente dal Sistema Informativo.
Nel caso un'utente del comune si assenti per un determinato periodo di tempo, il responsabile dei sistemi informativi è in grado di cancellare la password impostata dall'utente e di creare un nuovo id in modo da poter accedere alle risorse del PC.
In modo analogo l'amministratore del sistema è in grado di creare degli utenti temporanei per accedere agli

applicativi di business. Per cui la comunicazione delle password in busta chiusa seguirà le regole definite nella tabella del par 12.3.3.

12.3.4.1. Comunicazione di variazione delle password

Per quegli applicativi e strumenti elettronici il cui accesso è consentito esclusivamente tramite credenziali di autenticazione, la cui gestione e variazione non è riconducibile all'ufficio informatico, la stessa deve essere comunicata al custode delle password ogni qualvolta viene cambiata (vedi tabella paragrafo precedente). La copie delle credenziali di autenticazione vengono custodite in una busta chiusa archiviata in cassaforte dal responsabile dei sistemi informativi. Nel caso di assenza prolungata dell'incaricato del trattamento dei dati il responsabile dei sistemi informativi o un collaboratore del comune, previa autorizzazione del responsabile del trattamento, possono utilizzare le credenziali di autenticazione avvertendo l'incaricato dell'intervento effettuato.

12.3.5. Archivi documentali

Il comune di NOVENTA DI PIAVE tratta archivi documentali contenenti sia dati personali che sensibili che giudiziari.
Per quanto riguarda la gestione degli archivi cartacei l'ente ha adottato le seguenti regole:

- nel caso di documenti archiviati in armadi collocati in luoghi non presidiati dai dipendenti ed accessibili al pubblico, questi devono essere chiusi a chiave in modo da garantire la privacy e l'integrità delle informazioni contenute.
- dati personali archiviati in armadi dei vari uffici sono chiusi a chiave, nel caso ciò non sia possibile si provvede a chiudere a chiave l'ufficio.
- i **dati sensibili e giudiziari** necessariamente vanno custoditi in armadi dotati di serratura chiudibile a chiave.

Se durante le ore di lavoro, l'operatore del comune deve accedere ai documenti cartacei contenenti dati relativi ai cittadini del comune o dati relativi alla gestione dell'ente, gli stessi devono essere gestiti con attenzione in modo da non pregiudicarne la privacy o la sottrazione indebita. Al termine della consultazione gli stessi devono essere riposti con cura negli armadi da cui sono stati prelevati.
Nel caso alcuni documenti contenenti dati personali, sensibili o dati classificati come importanti non siano più utili questi devono essere distrutti in modo da non risultare leggibili.

La gestione dei documenti cartacei compete ai responsabili del trattamento dei dati ognuno per le proprie competenze.

12.3.5.1. Regole chiusura Uffici ed Armadi

Uffici

- al termine dell'orario di lavoro gli uffici devono essere chiusi;
- le chiavi sono in possesso ad almeno due persone dell'ufficio ed una depositata presso ufficio tecnico.

Armadi

- al termine della giornata lavorativa i documenti vanno riposti negli armadi;
- gli armadi vengono chiusi;
- le chiavi sono depositate in un armadio chiuso a chiave le cui chiavi sono a disposizione del responsabile e di almeno una persona all'interno del ufficio.

12.3.6. Archivi elettronici

I dati in formato elettronico sono custoditi su:

- floppy disk
- dischi ottici
- supporti magnetici

I supporti che contengono dati sensibili devono essere custoditi in un apposito locale ad accesso ristretto o in un armadio o cassetto chiuso a chiave.
Al termine dei loro utilizzo, quando non è più necessaria la conservazione, i supporti devono essere distrutti o cancellati da parte dell'incaricato previa autorizzazione del responsabile del trattamento dei dati competente.

12.4. Sistema Informativo

In questo capitolo viene descritto il sistema informativo del comune suddividendolo in:

- Server
- Impianto di rete
- Client
- Risorse software

12.4.1. Server

I server installati nel comune di NOVENTA DI PIAVE sono riportati nella tabella del par 10.2.1. Per ognuno di essi viene identificato il sistema operativo, il data base installato e la relativa banca dati elettronica. I server sono collegati ad un UPS che li alimenta nel caso di caduta della tensione elettrica.

12.4.2. Networking

La rete del comune di NOVENTA DI PIAVE è una rete Microsoft Windows 2003 server costituita da una Lan a cui accedono i client degli operatori. Dal punto di vista logico la rete si compone di un dominio a cui accedono gruppi di utenti diversi.
L'accesso alla rete viene gestito da un server di dominio che ne identifica criteri di protezione e politica di sicurezza. Tale server denominato Active Directory contiene una copia delle informazioni del dominio e convalida gli utenti. La protezione della rete locale da attacchi provenienti dall'esterno è stata realizzata installando un firewall. Lo scopo di questa apparecchiatura è quella di proteggere la LAN da attacchi esterni.
La sua attività è quella di bloccare il traffico sospetto proveniente da internet bloccando i pacchetti che contengono come indirizzo quello di una macchina interna.

12.4.3. Software

Nella tabella sotto identificata vengono elencati i software applicativi e di base attivati presso il Comune di NOVENTA DI PIAVE. Nella tabella per comodità sono anche identificati gli applicativi legati ad un contratto di assistenza.

Servizio	Software	Fornitore	Contratto di Manutenzione o servizio assistenza
Protocollo e Albo	Lotus Notes	SAGA SpA	Attivo
Delibere e Determine	Lotus Notes	SAGA SpA	Attivo
Bilancio	Sicra	SAGA SpA	Attivo
Economato ed Inventario	Sicra	SAGA SpA	Attivo
Tributi	Sicra	SAGA SpA	Attivo
Codici fiscali	Siatel	Ministero delle Finanze	Attivo
Servizi Demografici	Sicra	SAGA SpA	Attivo
Cittadini residenti all'estero	AnagAire	Ministero Interni	Attivo
Servizi sociali	File Office	Microsoft	Attivo
Rilevazione presenze	Time 2Win	SAGA SpA	Attivo
Polizia Locale	VisualPolcity	SAGA SpA	Attivo
Gestione Ufficio Tecnico	CnedWeb	Datapiano	Attivo
Programmazione Triennale		CEL srl	Attivo
Posta elettronica	Lotus Notes	SAGA SpA	Attivo
Biblioteca	TLM SoSeBi	SoSeBi	Attivo

12.4.4. Manutenzione del Sistema Informativo

Tra le prime cause di vulnerabilità dei sistemi hardware rientrano i guasti, il danneggiamento o anche il furto. Oltre a questi aspetti esistono altre modalità di danneggiamento dei sistemi che potrebbero essere: un incendio, gli sbalzi di tensione (spike) ecc. In questo paragrafo vengono identificate le misure adottate dal comune per la gestione delle apparecchiature, dei software applicativi e di sistema e per il mantenimento

delle stessi in uno stato di efficienza.

12.4.4.1. Manutenzione Hardware

I server, i personal computers gli apparati di rete e le stampanti in dotazione al comune di NOVENTA DI PIAVE, non sono coperti da contratto di manutenzione hardware. Le apparecchiature acquistate sono coperte da una garanzia on site della durata di tre anni con il costruttore.
Eventuali guasti, che necessitano l'intervento di una ditta specializzata, vengono affrontati di volta in volta con il coinvolgimento di ditte specializzate.
La maggior parte degli apparati di connessione alla rete di Internet prevede un contratto di locazione con Telecom Italia; la manutenzione di tutte queste apparecchiature è a carico della stessa. in quanto inclusa nel canone bimestrale. Il contratto di locazione scade al termine di ogni anno e viene automaticamente rinnovato.

12.4.4.2. Manutenzione Sistemistica

Attualmente non ci sono contratti in essere per gli aggiornamenti dei sistemi operativi, degli applicativi diagnostici o delle basi di dati. La gestione sistemistica viene fatta direttamente dall'ufficio informatico del comune.

12.4.4.3. Manutenzione degli apparati e del software

- **manutenzione preventiva: i**l responsabile del servizio informatico si occupa della manutenzione preventiva degli sistemi di base installati sui server. In particolare la persona incaricata della manutenzione preventiva si deve preoccupare di aggiornare il software di sistema installato sui server con le patch rilasciate dal produttore.
- **gestione assistenza del software:** per l'anno 2007 è stata assicurata l'assistenza software gli applicativi in essere nel sistema informatico comunale come indicato nella tabella riportata al punto 13.4.3.

12.5. Sicurezza delle Trasmissioni dei DATI

12.5.1. Trasmissione dei documenti cartacei

In questo paragrafo vengono identificate le regole per la trasmissione dei documenti cartacei nell'ambito del Comune di NOVENTA DI PIAVE.
Le regole adottate dall'ente prevedono:

- le comunicazioni in ingresso vengono protocollate dall'ufficio del protocollo, e i documenti classificati come riservati o contenenti dati sensibili vengono registrati a inoltrati all'ufficio competente come riservati;
- nel caso di comunicazioni verso l'esterno, la protocollazione della posta è gestita dai singoli uffici. La trasmissione di documenti che contengono dati sensibili prevede l'utilizzo della "doppia busta" Il documento contenente dati sensibili viene messo in una busta e accompagnato da una missiva con le indicazioni del destinatario senza riferimenti a dati classificati come sensibili.
- per la trasmissione di documenti tra uffici del comune, compresi lo smistamento della posta da parte del protocollo, deve rispettare una serie di principi in particolare quello di necessità e pertinenza. Cioè i dati possono circolare solo per ragioni di servizio e per la necessità dei singoli uffici. Inoltre la corrispondenza non deve passare indiscriminatamente da più persone evitando passaggi superflui. In particolare per la trasmissione di dati sensibili deve avvenire in busta chiusa, inoltre la corrispondenza che non può essere smistata deve essere custodita in armadi chiusi a chiave;
- il protocollo provvede alla conservazione informatica dei testi sia in entrata che in uscita, agganciati al numero di protocollo di riferimento; allo stesso modo procedono tutti gli uffici abilitati all'acquisizione dei numeri di protocollo in uscita.

12.5.2. Trasmissione Telematiche

Le reti sono un insieme di host tra di loro comunicanti. Le reti sono suddivise a seconda della dimensione. Si parla di rete LAN che copre una distanza ridotta solitamente all'interno di un edificio. Queste tipologie di reti servono per collegare uno o più server a dei client e a delle periferiche.
Si parla di WAN quando l'estensione della rete assume contorni geografici ampi e differisce dalla LAN anche

perché il controllo o la proprietà non è di un singolo ente.
Si parla poi di internet che è una rete di reti controllate da diversi società che supporta protocolli standard che consentono la comunicazione di utenti diversi. Le caratteristiche di internet si possono riassumere in questi tre punti:

Dimensione indeterminata: non è realmente possibile stabilire quale sia la dimensione di internet, identificare quanti siano il numero degli utenti;

Eterogenea i sistemi che si connettono ad internet hanno caratteristiche diverse tra di loro;

Esposizione fisica e logica dato che non esiste un controllo degli accessi globale qualsiasi persona può accedervi e grazie alla sua connettività può raggiungere qualsiasi risorsa della rete.

Questo fa capire quali siano i problemi e le minacce che possono derivare da internet. Le vulnerabilità che possono derivare dall'uso di questo sistema si possono identificare in una serie di aspetti:

- **anonimato** un malintenzionato può collegarsi ad internet e creare dei problemi ad un sistema che si trova a miglia di km di distanza stando dietro uno scudo elettronico. Infatti i sistemi di autenticazione tra i PC non è di tipo fisico come quello umano, ed inoltre un attacco può passare attraverso percorsi tortuosi usando centinai di host della rete.
- **presenza di numero esteso di punti di attacco:** quando un file od una informazione transitano da un pc ad un altro pc prima di raggiungere il destinatario transitano attraverso numerosi punti della rete. Questo implica che ci si deve "fidare" dei criteri di protezione e delle policy di accesso degli apparati intermedi.
- **complessità del sistema: i**nternet è un aggregato si hardware, software e sistemi operativi diversi. Ottenere una protezione affidabile risulta molto difficile in un sistema di questo tipo. Una rete può mettere in comunicazione due host con sistemi operativi diversi e questo può generare dei problemi sulla sicurezza.

12.5.3. Attacchi alla sicurezza

Senza la pretesa di offrire una classificazione formale e completa, possiamo considerare gli attacchi come violazioni delle proprietà di sicurezza precedentemente enunciate. I tipi di attacchi possono essere dunque:

- intercettazioni (violano la proprietà di segretezza dell'informazione);
- alterazioni (violano il requisito di integrità);
- generazioni (violano i requisiti di autenticità e di non-ripudio);
- interruzioni (minacciano la disponibilità del sistema).

Nella tabella sono elencate le caratteristiche principali di ogni categoria di attacco, insieme ad alcuni esempi presi da contesti reali.

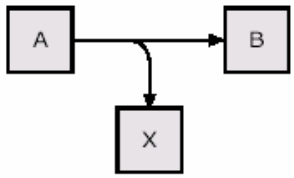
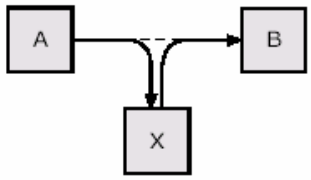
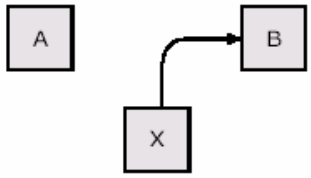
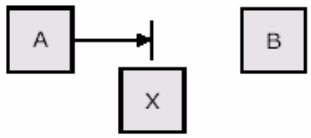
Attacco	*Schema*	*Esempi del mondo reale*
Flusso normale dell'informazione		Invio di un pacchetto IP Invio di email Accesso a una pagina web Lettura di dati da un database
Intercettazione		Sniffing di pacchetti di rete Furto di informazione mediante crittoanalisi Furto di informazione mediante analisi del traffico Furto di informazione mediante covert channel
Alterazione		Modifiche non autorizzate a file o programmi Attacchi man-in-the-middle Azioni di disturbo nel canale di comunicazione
Generazione		Masquerading Spoofing Intrusioni
Interruzione		Denial of service Flooding, resource starvation, mail storm Crashing di applicazioni Sabotaggio linee di comunicazione Danneggiamenti fisici

Tabella 1 – Le principali categorie di attacchi alla sicurezza informatica.

12.5.4. Sicurezza della rete

La rete consente alle varie stazioni di lavoro di collegarsi alle unità centrali di elaborazione dei dati. Una rete locale mediante opportuni apparati si può poi collegare ad internet, è intuitivo che i livelli di protezione del sistema informativo cambiano se si verifica quest'ultima condizione.

La rete del comune di NOVENTA DI PIAVE è configurata mediate la definizione di un dominio a cui accedono gruppi di utenti previa autenticazione. Per quanto riguarda la rete locale la politica di gestione degli indirizzamenti prevede l'utilizzo di uno schema di indirizzi IP che utilizzano il servizio DHCP.

12.5.5. Connessioni dial-up

Le connessioni via modem tra la rete dei Sistema Informatico Comunale con reti e/o sistemi esterni possono rappresentare un serio rischio per il Sistema stesso. Come conseguenza di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga a rischio l'intero sistema informativo ed i dati in esso contenuti. Ciò può avvenire senza che il dipendente se ne renda conto.
Per tale motivo ogni collegamento dall'interno verso l'esterno e viceversa deve rispettare i criteri di sicurezza qui esposti e quelli che verranno stabiliti dal Ced.
Di norma i modem collegati alle workstation devono restare spenti se non utilizzati.
Tutti gli accessi alla rete esterna, devono essere effettuati tramite una connessione protetta da Firewall; accessi tramite Remote Access Server (RAS) non sono permessi.

Accessi tramite modem per la teleassistenza attraverso una linea telefonica possono essere effettuati purché non si tratti di una connessione ad internet.

12.5.5.1. Connessioni per Assistenza Remota

Il collegamento con le software house che devono connettersi al sistema informativo del comune per fare assistenza in modalità remota avviene utilizzando il software "VNC" e la connessione ADSL internet in sola uscita (non compromettendo, in questo modo, la sicurezza). Attraverso questo tool è il cliente stesso che "cede" il controllo della propria macchina alla ditta che deve fare assistenza potendone osservare le attività che vengono fatte sulla stessa. Questa forma esplicita di collegamento da parte dell'utente permette un controllo sufficiente della sicurezza della rete.

12.5.6. Internet

Il rischio connesso al collegamento a Internet della rete locale è quello di consentire a soggetti terzi di entrare ed operare nella LAN e acquisire, modificare o distruggere risorse importanti come i dati in essa contenuti.
Il controllo della sicurezza viene mantenuto centralmente dal Ced attraverso l'impostazione di una serie di misure minime volte a migliorare l'efficienza del sistema.
Uno degli strumenti attivati nel comune di NOVENTA DI PIAVE, per evitare che siano possibili accessi indiscriminati ai dati privati, è costituito da firewall, attraverso il quale tutti i computer della rete accedono a Internet e viceversa, così che sia possibile impostare dei criteri per accettare o rifiutare le diverse connessioni.
L'apparato consente di effettuare un primo filtro e segnala in tempo reale attività relativi ad accessi sospetti. L'informazione di log consente di tracciare tutti gli accessi sospetti e di prendere le contromisure che l'amministratore ritiene opportuno attuare.

12.5.7. Virus

I virus informatici sono dei programmi che possono causare dei guasti consistenti ai dati o ai programmi. I virus possono attaccare i file eseguibili e le macro contenute nei programmi di elaborazione dei dati. Molti virus possono essere introdotti nel sistema tramite dischi floppy o collegandosi ad Internet. Una buona forma di difesa da questi attacchi consiste nel definire delle limitazioni al down load dei programmi ma anche un attento utilizzo delle potenzialità dei servizi offerti dal sistema informativo. A tale scopo è stato diffuso un decalogo contenete delle indicazioni sul buon uso delle risorse del sistema informativo, con lo scopo di sensibilizzare l'utente di fronte alle possibili tecniche di diffusione dei virus e quindi agli accorgimenti da attuare quando si presentano determinati eventi quali:

- messaggi di posta di cui non si conosce la provenienza
- messaggi di posta che contengono file eseguibili
- supporti magnetici da cui leggere determinati file ecc.
- accessi a siti di dubbia qualità

Altri elementi attuati per aumentare la sicurezza da virus sono:

- limitare l'installazione di software che vengono scaricati da internet in modo che gli utenti non possano danneggiare l'efficienza e il funzionamento del sistema installando del sw di dubbia provenienza.
- istruzione agli utenti al fine di controllare i supporti usati per lo scambio di dati o di file prima di utilizzarli.

La responsabilità di verificare che l'aggiornamento dell'antivirus avvenga automaticamente è dell'utilizzatore dei personal computer, in caso contrario deve essere lanciato manualmente upgrade della suite antivirus.

12.5.8. Software antivirus

Il comune di NOVENTA DI PIAVE dispone di un sistema antivirus, le cui caratteristiche di base sono di seguito elencate:

1. gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite Internet;
2. deve essere particolarmente efficace contro i virus della nostra area geografica;
3. deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma;
4. deve poter effettuare una scansione automatica del floppy disk;
5. deve essere in grado di effettuare scansioni a intervalli regolari e programmati;

6. deve essere in grado di effettuare la scansione all'interno dei file compressi;
7. deve mantenere il livello di protezione in tempo-reale;
8. deve eseguire la scansione in tempo-reale;
9. deve poter eseguire la rimozione del codice virale in automatico;
10. predefinita (quarantena);
11. deve essere attivo nella protezione per Applet di ActiveX e Java contenenti codice malizioso;
12. deve essere in grado di effettuare la rilevazione/pulizia dei virus da Macro sconosciuti;
13. deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo.

Il sistema attivato opera in modo complementare su due livelli.

- **antivirus di posta:** in particolare un sw antivirus è installato sul server che pubblica la posta attraverso web. Un sistema ativirus specifico per la posta è installato sui server Linux che gestisce la posta elettronica.
- **antivirus a bordo macchina (client/Server):** un sw antivirus è installato sui server del SI del comune e sui client. L'aggiornamento dell'antivirus avviene in modo automatico attraverso una procedura di script che si suddivide in due moduli:
    1. Verifica del collegamento tra server su cui è installato l'antivirus e client della rete.
    2. Script che aggiorna il client nel caso il sw installato abbia una versione superata.

Il prodotto è coperto da contratto di assistenza che annualmente viene rinnovato e che consente di aggiornare la suit con le nuove impronte virali messe a disposizione dal produttore.
I sw antivirus sono continuamente aggiornati attraverso la stipulazione di un contratto di assistenza con al sw house che lo produce.

12.5.9. Software Antispam

Previsto nel contratto di servizio di posta elettronica fornito dalla Provincia di Venezia.

12.6. Criteri per il Ripristino della Disponibilità dei Dati

12.6.1. Copie dei Dati

Il sistema informativo è strutturato con delle unità di copia a nastro attraverso la quale vengono fatti i backup dei dati presenti sui server e delle tabelle di sistema.
Al personale del comune sono state inviate delle istruzioni per il salvataggio dei propri file in cartelle ad accesso esclusivo create sul file server, in modo tale che possano essere effettuate le copie dei dati di interesse su supporti removibili.
Le copie vengono fatte giornalmente attraverso una procedura schedulata di notte.
Esistono note operative da seguire per la effettuazione il controllo sul esito delle operazioni di back-up a disposizione di chi si occupa della procedura.
I supporti utilizzati per ciascun server sono 5, uno per ogni giorno della settimana dal lunedì al venerdì e riutilizzate a rotazione.
Le unità di back-up sono conservate negli uffici del ced in un armadio chiuso a chiave. Le cassette del fine settimana vengono conservate in una cassaforte ignifuga presso la sala CED.
Periodicamente una unità di backup viene depositata presso la cassetta di sicurezza del tesoriere.

Data Base	Procedure di salvataggio	Ubicazione conservazione delle copie	Struttura incaricata del salvataggio
Sicra - SQL	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico
Lotus Notes	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico
VisualPolcity	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico
Time 2Win	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico
Cnedweb	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico
TLM SoSeBi	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico
Posta elettronica	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico
File di produttività individuale	Schedulata	Cassaforte Ignifuga Sala Server	Sistema Informatico

12.6.2. Riutilizzo controllato dei supporti

I PC dismessi vengono catalogati e conservati presso ufficio informatico del comune di NOVENTA DI PIAVE previa cancellazione di tutti i dati in essi registrati. Esistono norme interne per il riutilizzo dei supporti nei quali eventualmente erano stati registrati dati di cui agli artt.22 e 24 dell'allegato B.

12.6.3. Disaster Recovery

L'implementazione di un piano della sicurezza relativo ai sistemi informativi deve tenere conto della necessità di ripristinare, in un determinato intervallo di tempo, le condizioni di funzionamento esistenti prima del verificarsi del guasto o dell'attacco. Il tempo di interruzione del servizio sopportabile dipende dalla criticità che riveste lo stesso e non può andare oltre i 7 giorni. Nel caso del Comune di NOVENTA DI PIAVE allo stato non sono state previste soluzioni di alta affidabilità. Il piano di continuità prevede le seguenti fasi:

- il responsabile del Back-up archivia giornalmente la cassetta di copia dei dati del comune nella cassaforte in sala server. Oltre ai dati i nastri contengono una copia delle configurazioni di dominio dell'ente;
- nello stesso luogo sono archiviate le copie, su supporto ottico, dei sistemi operativi e degli applicativi installati sui server e le istruzioni per il restore dei dati e delle configurazione di sistema;
- una cassetta con il back-up di fine settimana viene conservata in una cassetta di sicurezza presso una banca.

Nel caso di disastro che danneggia gravemente il sistema informativo del comune il responsabile dei sistemi informativi provvede a ripristinare il funzionamento delle apparecchiature guaste facendo intervenire delle ditte specializzate.
Una volta predisposto l'hardware si procede al restore dei dati di sistema, successivamente si installano gli applicativi software e si procede con il restore dei dati di business.

13. FORMAZIONE

La gestione della sicurezza informatica in una qualsiasi organizzazione vede coinvolte in modo stretto gli utenti del sistema. Ciò richiede un piano di formazione rivolto ad ogni dipendente che utilizza le risorse informatiche dell'organizzazione. L'obbiettivo è quello di creare la "cultura della sicurezza" attraverso una serie di attività volte ad illustrare i provvedimenti ed i comportamenti da adottare per migliorare la sicurezza nel trattamento dei dati. il piano è stato studiato, organizzato e suddiviso sulla base delle specifiche esigenze di ciascuna area in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati, nonché dei criteri e delle modalità di evitare tali rischi.

Periodicamente il responsabile dei sistemi informativi del Comune trasmette a tutti i dipendenti del materiale informativo in cui sono riportate le principali regole di gestione ed utilizzo delle risorse del sistema informativo.

13.1. Piano di formazione

Per tutte le risorse umane, che svolgono trattamenti di dati personali, è stata pianificata un'attività formativa avente l'obiettivo di renderle edotte sui rischi possibili o probabili al fine di prevenirli. I contenuti essenziali sono:

- informazioni sulla legge 196/2003 testo unico sulla Privacy.
- contenuti delle principali leggi in materia di sicurezza informatica (Leggi n. 547/93 e 518/92);
- principi legislativi e comunitari
- funzionamento della normativa nell'ambito dei diritti del cittadino
- crimini informatici, frodi, abusi, danni, casistica
- rischi possibili e probabili cui sono sottoposti i dati
- misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi
- comportamenti e modalità di lavoro per prevenire i rischi

Tale formazione viene erogata mediante supporti informativi cartacei, elettronici e/o telematici.

Il piano di formazione verrà erogato anche per i dipendenti neo assunti che nell'ambito delle loro mansioni svolgono trattamento dei dati.

14. GESTIONE DEI SERVIZI FATTI DA SOCIETA' ESTERNE

Il comune di NOVENTA DI PIAVE affida ad alcuni fornitori la gestione di alcuni servizi quali la manutenzione delle apparecchiature e delle facility relative alla sala ced; la gestione dell'assistenza degli applicativi software installati presso il comune e servizi di connessione e di service provider. Questo implica che collaboratori di queste aziende possano trattare parzialmente dati ed informazioni gestite dal Comune. A tale proposito il comune ha nominato queste aziende responsabili del trattamento dei dati nell'ambito del loro operato.

14.1. Servizi dati in outsourcing

Nella tabella sottostante sono state identificate le aziende che gestiscono in outsourcing servizi per il comune di NOVENTA DI PIAVE.

Servizio	Tipologia di Dati	Fornitore	Comunicazione Responsabilità Trattamento dei dati
Manutenzione sistema informativo	Banche dati del comune relative a Demografico, Affari generali, Ragioneria, Polizia Locale, Presenze	Sesa Informatica	Sesa Informatica Galleria Spagna Padova
Manutenzione Software Biblioteca	Banche dati del comune relative a Demografico, Affari generali, Ragioneria, Polizia Locale, Presenze	SoSeBi	SoSeBi Srl Via dell' Artigianato 9 09122 Cagliari
Servizi ISP	Posta Elettronica	Provincia di Venezia	
Tesoriere	Gestione anagrafiche e pagamenti	Cassa di Risparmio di Venezia	Via Vizzotto San Donà' di Piave (VE)
Lampade Votive	Gestione anagrafiche e pagamenti	Marzaro Impianti	Via Provinciale Sud, 61 Cazzago di Pianiga (VE)
Concessionaria Pubblicità	Anagrafica Utenti Imposta sulla Pubblicità e pubbliche affissioni	Duomo GpA Srl	P.zza Garibaldi, 40 CODROIPO (UD)
Gestione Ruoli Coattivi	Anagrafica Utenti Importo ruoli	Equitalia	Equitalia
Scansioni dichiarazioni ici	Banca dati dell'ICI	Work way	Work way srl Treviso viale Felissent 84/D Treviso
Accertamento rendite catastali	Banca dati dell'ICI	Studio ing Emilio Rizzini	Via A Franchetti 110 Vicenza
Cedolini paghe	Anagrafica dipendenti, posizione reddittuale e contributiva.	Consorzio OpiterGino	Via degli Alpini, 10 Oderzo (TV)
Gestione Inventario	Dati beni mobili ed immobili	GIES srl	Repubblica di San Marino
Registro Tumulazioni		Il Bozzolo Verde	San Donà di Piave

Il contratto relativo alle soluzioni software copre gli aggiornamenti di Legge e la soluzione dei malfunzionamenti riscontrati.
Per gli altri software non sono stipulati altri contratti ed eventuali malfunzionamenti vengono affrontati dagli addetti del ced o con l'intervento di aziende esterne.

15. Audit della Sicurezza

15.1. Verifiche generali

Le verifiche sulla corretta applicazione delle misure di sicurezza generiche per la protezione dei dati e delle informazioni gestite dal comune nel suo complesso e delle misure particolari in riferimento esplicito a quelle previste dalla legge sul trattamento dei dati personali, sono affidate all'Agenzia Informatica che si avvale di apposite liste di controllo.
Le singole funzioni sono comunque tenute alle verifiche previste nella tabella di sintesi sotto riportata.

MISURE DA VERIFICARE	OGGETTO DELLE VERIFICHE	CADENZA	RESPONSABILE
Organizzazione			
Aggiornamento DPS	Controlli periodici, ed aggiornamento del DPS	Annua Entro 31/3	Maschietto Donatella Scaramal Michele
Outsourcing	Verifica criteri di sicurezza dei fornitori	a Campione	Responsabili di P.O.
Incarichi inerenti la sicurezza ed il trattamento dei dati	Controlli periodici degli incarichi, dei compiti e delle responsabilità.	Annua	Responsabili di P.O.
Analisi dei rischi	Analisi dei rischi e delle contromisure da adottare per contrastarli.	Annua	Scaramal Michele
Autorizzazioni all'accesso	almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione	Annua	Scaramal Michele
Autorizzazioni all'accesso	Rilasciate e revocate periodicamente	Sempre	Scaramal Michele
Piano di formazione	Attivazione del piano di formazione per nuovi collaboratori del comune	Sempre	Maschietto Donatella
Protezione fisica			
Protezione delle aree e dei locali	controlli periodici degli impianti e dei sistemi di sicurezza	Annua	Responsabile ufficio tecnico
Antincendio	Manutenzione periodica secondo le indicazione dell'installatore		Responsabile ufficio tecnico
UPS	Manutenzione preventiva UPS Secondo le istruzioni del costruttore.		Scaramal Michele
Controllo accessi fisici ai locali	controlli periodici dei sistemi che regolano l'accesso agli edifici, agli archivi o alle aree ad accesso ristretto.	Annua	Amorino Giurato
Protezione Logica			
Criteri e procedure per assicurare l'integrità dei dati	Controlli accessi banche dati. Controllo utilizzo modalità di autenticazione	Annua	Scaramal Michele
Codici identificativi personali	disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore	Sempre	Scaramal Michele
Restrizioni di accesso per via telematica	Controllo account sistema informativo	Annua	Scaramal Michele
Sicurezza delle trasmissioni dei dati	controlli periodici log dei firewall	mensile	Scaramal Michele
Sistema Informativo			
Antivirus	Verifica buon funzionamento	Annuale	Scaramal Michele

	Verifica aggiornamento		
Patching	Aggiornamento periodico dei sistemi informativi dei server Aggiornamento periodico dei sistemi informativi dei client	Ogni mesi	Scaramal Michele
Back-up Dati	Verifica back-up dei dati e dei dati di sistema e efficienza apparecchiature e supporti.	quotidiana	Scaramal Michele
Re impiego dei supporti di memorizzazione	Controlli sulla recuperabilità delle informazioni precedentemente contenute	Sempre	Scaramal Michele