COMUNE DI CALUSO
Provincia di Torino
Settore amministrativo e dei servizi alla persona

Caluso città viva

ALLEGATO 06

al Manuale di Gestione del Protocollo informatico, dei documenti e dell'Archivio del Comune di CALUSO

PIANO PER LA SICUREZZA

Riferimenti normativi

Il "piano per la sicurezza informatica" riporta le misure minime di sicurezza, organizzative e tecnologiche, messe in atto dal Comune di Caluso.

Il presente documento è il Piano per la Sicurezza ai sensi del Codice dell'Amministrazione Digitale (D.Lgs n. 82 del 7 marzo del 2005), del testo Unico 445/200 e del D.Lgs. 196/2003.

Definizioni

Trattamento di dati: si intende, qualunque operazione o complesso di operazioni, effettuati con l'ausilio di strumenti elettronici, concernenti: la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati (art.4 del D.Lgs. 196/2003).

Dati sensibili: dati personali idonei a rivelare l'origine *razziale* ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a 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: dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 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: persona fisica o giuridica o altro organismo cui competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, compreso il profilo della sicurezza.

Responsabile del trattamento: persona fisica o giuridica preposta dal titolare al trattamento dei dati personali.

Incaricato: persona fisica identificata tramite apposita nomina del Responsabile del trattamento che esegue le operazioni di trattamento.

La nomina degli incaricati del trattamento rientra tra le competenze dei predetti Responsabili del trattamento.

Addetti alla custodia delle parole chiave: persone incaricate della custodia delle parole chiave di accesso ad informazioni o di accedere alle stesse.

Amministratore di sistema: soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo e/o di gestione dei data base e di consentirne l'utilizzazione.

Nel Comune di Caluso è individuato nel soggetto esterno incaricato della gestione del sistema informatico.

Incaricati della manutenzione: persone addette alla manutenzione dell'hardware, del software applicativo e del software di base degli elaboratori sui quali sono memorizzati i dati personali.

PDL: postazione di lavoro.

HOST - Server: con HOST si identificano le macchine fisiche che ospitano i Server, ovvero le macchine virtuali che svolgono funzioni informatiche od ospitano gli applicativi software.

Introduzione

L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è anche quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.
Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, i software applicativi, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, di gestione documentale, di protocollazione e conservazione digitale a norma etc.
Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.
L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e responsabili di settore) dell'Amministrazione ed i loro interlocutori.
È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

Scopo

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione in ogni suo aspetto. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

Ambito di applicazione

Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, stagisti, ...), includendo tutto il personale affiliato con terze parti. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

Politiche di sicurezza

1. Disciplinare interno per un corretto utilizzo degli strumenti informatici della posta elettronica e per la navigazione in internet (Allegato 6.1).
2. Specifiche di Backup attuate nell'ente (Allegato 6.2).
3. Studio di fattibilità tecnica relativo al piano di continuità operativa e disaster recovery (Allegato 6.3).

Allegato 6.1)

Disciplinare interno per un corretto utilizzo degli strumenti informatici della posta elettronica e per la navigazione in internet

PRINCIPI GENERALI

1. Il presente documento, emanato in riferimento alle leggi D.Lgs 196/2003 e al D.Lgs n. 82/2005 e smi., costituente allegato al Manuale di Gestione del Protocollo, contiene la disciplina precedentemente inclusa nel Documento per la sicurezza la cui adozione è stata abolita dal DL 9/2/2012, n. 5 – L. 4/4/2012, n. 35 senza comunque far venir meno in capo al Titolare del trattamento dei dati l'obbligo di garantire l'osservanza delle misure minime di sicurezza.
2. La violazione del presente disciplinare potrà comportare l'applicazione delle sanzioni disciplinari contemplate dal Contratto collettivo nazionale di lavoro applicabile, nel rispetto dei principi di gradualità e proporzionalità, nonché delle altre misure di tutela del caso.

USO DEGLI STRUMENTI INFORMATICI E MISURE DI SICUREZZA

3. Il personal computer e gli altri strumenti elettronici eventualmente assegnati o a disposizione degli incaricati costituiscono strumento di lavoro.
Pertanto l'utilizzo di essi da parte degli incaricati è consentito esclusivamente per finalità direttamente attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative ed interne, comunque con esclusione di qualsivoglia uso per scopi privati e/o personali.
4. L'utilizzo di tali strumenti non configura alcuna titolarità, da parte dell'incaricato, dei dati o delle informazioni trattate, che appartengono al Comune di Caluso ed ai quali il dipendente si riserva pertanto, nei limiti consentiti dalle norme legali e contrattuali, il diritto di accedere.
5. Il personal computer, e gli altri eventuali strumenti elettronici, sono affidati dal Comune di Caluso all'incaricato, con ogni conseguente obbligo di custodia e di utilizzo appropriato. L'incaricato è tenuto ad informare immediatamente il Comune di Caluso nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli stessi, del sistema o del software installato, utilizzando i sistemi di comunicazione di volta in volta indicati.
6. L'incaricato deve utilizzare gli strumenti elettronici con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza. Per quanto possibile gli strumenti sono configurati in modo da garantire il rispetto delle regole descritte nel presente disciplinare; tale configurazione non deve essere mutata. Ogni anomalia o disfunzione deve essere prontamente segnalata al Comune di Caluso.
7. L'accesso al sistema operativo del personal computer, o degli altri strumenti elettronici, è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password). Per l'uso, la scelta, la modifica di tali credenziali si rinvia a quanto previsto dalle istruzioni e dalle procedure.
Si rammenta che il nome utente è assegnato all'incaricato dal Comune di Caluso e la password deve essere scelta e registrata dall'incaricato nel rispetto di quanto previsto dalle norme, dalle procedure e dalle istruzioni, deve essere mantenuta segreta ed in nessun caso può esserne consentito l'uso a terzi.
8. L'incaricato è tenuto a modificare la propria password, nel rispetto dei criteri previsti dalle norme e dalle istruzioni ricevute. In ogni caso, l'incaricato è tenuto a modificare la propria password, anche prima del decorso dei giorni previsti dall'ultima modifica, e comunque nel rispetto dei criteri suddetti, allorché ritenga che altri possa in qualsiasi modo esserne venuto a conoscenza o che possa comunque esserne venuta meno la

segretezza. La password dovrà essere variata dall'incaricato entro i termini massimi, sia se il sistema è temporizzato con conseguente blocco dell'accesso al personale computer e/o al sistema in caso di mancata variazione, sia se non lo è.
9. Il Comune di Caluso assicura la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
10. Non è consentito installare sui personal computers o sugli strumenti elettronici software, anche se gratuiti, non distribuiti e/o comunque non espressamente autorizzati dal Comune di Caluso, né collegare ai personal computer o agli strumenti elettronici periferiche hardware o dispositivi non messi a disposizione dal Comune di Caluso.
11. Non è consentita la modifica delle impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, del software di posta elettronica e di ogni altro software installato sui personal computer o sugli strumenti elettronici o sul sistema.
12. Non è consentito caricare o comunque detenere nei personal computer o negli strumenti elettronici materiale informatico, dati ed informazioni personali o comunque di contenuto non attinente alla mansione ricoperta.
13. È in ogni caso tassativamente vietato caricare o detenere materiale informatico:
a) il cui contenuto (a mero titolo esemplificativo: testo, audio e video) sia coperto da diritto d'autore;
b) il cui contenuto attenga o riguardi dati sensibili (salvo che si tratti di dati che è indispensabile trattare con tali mezzi,conformemente alle disposizioni ed istruzioni, per le mansioni attribuite) o che consenta di conoscere dati sensibili;
c) il cui contenuto sia contrario a norme di legge e/o comunque per finalità ludiche o di svago.
14. Non è consentito agli incaricati impostare protezioni o password ulteriori rispetto alle credenziali di autenticazione predisposte dal Comune di Caluso che limitino l'accesso al personal computer, agli strumenti elettronici e/o alle relative periferiche (esempio impostare password a livello di BIOS).
15. L'incaricato deve:
a) spegnere l'elaboratore, gli altri strumenti elettronici ed eventuali periferiche direttamente collegate (stampanti; scanner ecc.) prima di lasciare l'ufficio al termine dell'attività lavorativa o in caso di allontanamenti protratti dal posto di lavoro e deve comunque adottare le altre cautele previste dalle procedure/istruzioni, anche in caso di brevi allontanamenti;
b) far eseguire le operazioni di manutenzione/riparazione degli strumenti solo da parte del personale autorizzato dal Comune di Caluso;
e) evitare, senza preventiva autorizzazione, qualsiasi uso di strumenti elettronici personali (pc, periferiche,dispositivi di memorizzazione, ...) sul luogo di lavoro o per usi lavorativi;
d) non modificare o disattivare in alcun modo la funzione di screen saver con password della propria postazione di lavoro;
e) non alterare o disattivare le altre misure di sicurezza minime od ulteriori adottate dal Comune di Caluso ed anzi effettuare quanto di competenza per garantirne il funzionamento, segnalando tempestivamente ogni anomalia o disfunzione;
f) non impostare password o analoghe protezioni ai singoli archivi informatici (dischi, cartelle o files), al di fuori di quelle previste dalle procedure interne, dalla configurazione del sistema, o da specifiche istruzioni scritte.
16. Tutta la gestione degli strumenti elettronici, incluse le modifiche alla configurazione dei sistemi desktop e portatili, può essere effettuata unicamente dal Comune di Caluso o da soggetti espressamente e formalmente autorizzati. Gli incaricati non sono autorizzati a modificare il sistema neppure se si tratta della postazione di lavoro

assegnata.
17. È vietato il salvataggio, sia per scopi personali che per scopi professionali, dei dati personali di qualsiasi natura sugli hard disk del PC;
18. Le cartelle utenti presenti nei server del Comune di Caluso sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.
Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
Su queste unità vengono svolte regolari attività di verifica, amministrazione e back up da parte del personale incaricato.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali non sono soggette a salvataggio automatico. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo incaricato.
19. Il personale incaricato può in qualunque momento procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.
20. Con regolare periodicità dal back up si provvede in modo automatico alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili.
21. Gli incaricati sono tenuti a prendere visione della documentazione in materia di privacy e sicurezza dei dati resa disponibile dal Comune di Caluso in via informatica o cartacea e a darvi integrale applicazione.
22. Al fine di garantire l'integrale rispetto delle norme relative al corretto utilizzo del PC e degli strumenti elettronici, il Comune di Caluso si riserva di disporre ed effettuare controlli occasionali in conformità alle norme vigenti, secondo quanto previsto nel presente disciplinare.

UTILIZZO DELLA RETE INTERNET
23. L'accesso alla Rete internet costituisce esclusivamente risorsa dell'ente e strumento di lavoro. Pertanto l'utilizzo di internet da parte degli incaricati è consentito unicamente per finalità direttamente attinenti o comunque connesse all'esercizio delle mansioni attribuite e alle attività di pertinenza, con esclusione di qualsivoglia uso per scopi privati.
24. È proibito entrare nella rete e nei programmi con un codice d'identificazione diverso da quello assegnato. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno gestite secondo le istruzioni ricevute.
25. È vietato scaricare (download) dalla Rete internet:
a) software senza previa verifica dell'attendibilità dei siti in questione;
b) software non distribuiti e/o comunque non espressamente autorizzati dal Comune di Caluso;
c) materiale informatico, file o software non direttamente attinenti all'esercizio delle mansioni attribuite e alle attività di pertinenza;
d) materiale informatico, file o software il cui contenuto (a mero titolo esemplificativo: testo, audio e video) sia coperto da diritto d'autore, eccetto nei casi in cui ciò sia necessario per la propria attività lavorativa (es: testi, banche dati ecc.). Anche in tale caso l'incaricato è tenuto a verificare il diritto di proprietà del materiale, ad attivare gli eventuali adempimenti, prima di procedere al download, sentito il responsabile del trattamento e comunque a rimuovere immediatamente il materiale non autorizzato.
26. Non è consentito:
a) la partecipazione a forum di discussione online o chat o similari per ragioni non direttamente attinenti o connesse all'attività lavorativa;
b) l'utilizzo di chat line o di sistemi di chiamata o videochiamata (VoIP o similari) di

bacheche elettroniche e gli accessi da utenti "ospiti" (*guest*) neppure utilizzando pseudonimi (o nicknames);
c) la navigazione in internet su siti nei quali vi sia trattamento di dati sensibili o la navigazione nei quali possa in alcun modo comportare il trattamento di dati sensibili;
d) la navigazione in internet su siti contrari a norme di legge, a titolo esemplificativo di contenuto erotico o pornografico e/o comunque per finalità ludiche o di svago;
e) accedere a siti e/o forum, chat ecc. sotto il nome altrui, dovendo sempre, al contrario, utilizzare il proprio nome;
f) navigare e registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
g) l'effettuazione di transazioni finanziarie quali: acquisti on-line, trading on line e simili, fatti salvi i casi direttamente ed espressamente autorizzati dal titolare e comunque nel rispetto delle normali procedure di acquisto;
27. In un'ottica preventiva, il Comune di Caluso si riserva di provvedere:
a) a predisporre un sistema informatico di filtraggio teso ad impedire la navigazione su determinati siti web considerati non sicuri o comunque non pertinenti all'attività lavorativa;
b) a configurare/predisporre sistemi o filtri che prevengano determinate operazioni reputate non correlate con l'attività lavorativa, quali l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dati).
28. Tuttavia, poiché l'utilizzo di filtri, considerata la vastità della Rete internet e la sua continua evoluzione, non può garantire il corretto utilizzo della Rete internet da parte degli incaricati, né che sia impedito l'accesso ad ogni sito web non sicuro o non pertinente all'attività lavorativa, il Comune di Caluso si riserva di disporre ed effettuare controlli occasionali in conformità con quanto previsto dalle norme e dal presente, anche tramite l'esame dei file di log relativi al traffico web, finalizzate all'integrale rispetto delle misure di sicurezza e del presente disciplinare.
29. Gli incaricati debbono segnalare ogni anomalia, vulnerabilità o disfunzione che dovesse verificarsi nella navigazione sulla Rete internet.
30. Al fine di garantire l'integrale rispetto delle norme relative al corretto utilizzo della Rete internet, il Comune di Caluso si riserva di disporre ed effettuare controlli periodici e occasionali in conformità alle norme vigenti, secondo quanto previsto nel presente disciplinare.

UTILIZZO DELLA POSTA ELETTRONICA
31. Il Comune di Caluso mette a disposizione degli incaricati il servizio di posta elettronica assegnando a ciascuno di essi caselle di posta istituzionali per fini esclusivamente lavorativi.
32. Inoltre, al fine di agevolare lo svolgimento dell'attività lavorativa, il Comune di Caluso ha reso disponibili indirizzi di posta elettronica condivisi tra più incaricati (come, ad esempio, caselle di posta istituite per singole unità organizzative), affiancandoli a quelli individuali.
33. L'indirizzo di posta elettronica messo a disposizione degli incaricati dal Comune di Caluso, contraddistinta dalla presenza del nome di dominio "Comune di Caluso", costituisce esclusivamente uno strumento di lavoro. Pertanto, l'utilizzo della stessa da parte degli incaricati è consentito unicamente per finalità direttamente attinenti o comunque connesse all'esercizio delle mansioni attribuite e alle attività di pertinenza.
34. La corrispondenza elettronica in uscita verso l'esterno della rete comunale può contenere a pie di pagina, qualora previsto dalla normativa vigente, il disclaimer sulla riservatezza della comunicazione nonché l'indicazione della natura professionale, e non personale, del messaggio; i personal computer possono essere configurati in modo da

generare automaticamente il relativo testo su tutta la corrispondenza in uscita. Gli incaricati sono tenuti a verificare l'eventuale presenza delle indicazioni a pie di pagina.
35. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dall'incaricato nel rispetto dei criteri indicati e di quelli previsti dalle procedure/istruzioni e disposizioni. La sicurezza e la riservatezza dei file di archivio della posta elettronica in entrata e in uscita sono garantite dal sistema di protezione del Comune di Caluso; pertanto, non è consentito agli incaricati impostare altre credenziali o analoghe protezioni ai file di archivio della posta elettronica in entrata e in uscita.
36. Al fine di un corretto utilizzo della posta elettronica:
a) è vietato:
I utilizzare la posta elettronica per scopi personali e comunque per inviare o ricevere software o materiale informatico o dati o informazioni di qualsiasi tipo per scopi personali, o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list per attività non attinenti all'espletamento della propria mansione professionale;
II la redazione, l'invio o lo scambio e l'archiviazione di messaggi di posta elettronica contenenti dati sensibili o giudiziari o idonei a rivelare dati sensibili o giudiziari, salvo che ciò sia necessario per l'espletamento delle proprie mansioni, nel qual caso si potrà procedere solo a seguito di espressa autorizzazione previa adozione delle misure e cautele previste dalle norme o dalle istruzioni o dalle procedure;
III la partecipazione a catene telematiche (o di Sant'Antonio), se dovessero peraltro essere ricevuti messaggi di tale tipo, ciò dovrà essere comunicato immediatamente al Servizio Comunale compente. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
IV l'invio o la memorizzazione di messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria per sesso, razza, lingua, religione, origine etnica, opinione ed appartenenza sindacale e/o politica, contrari a norme di legge, alla decenza o al pudore, o comunque di contenuto oltraggioso o in ogni altro modo idonei ad offendere, nonché di messaggi a catena e/o spam;
V l'uso di linguaggio o di immagini oscene, ingannevoli, diffamatorie, discriminatorie e/o comunque suscettibili di creare un danno al Comune di Caluso o a terzi;
VI lo scambio di messaggi sotto mentite spoglie, ossia impersonando un mittente diverso da quello reale;
VII inviare o ricevere o scambiare messaggi di posta (con o senza allegato) contenenti:
1) immagini, filmati, e qualunque tipo di file dai contenuti illegali, violenti e/o pornografici;
2) file (o materiali informatici) soggetti al diritto d'autore (file musicali, video o eseguibili di programma, ad es. mp3 e ecc.) o eseguibili;
3) link a siti con contenuti illegali, violenti e/o pornografici, o comunque idonei a rivelare dati sensibili;
4) password e/o codici di accesso a programmi soggetti a diritto d'autore e/o a siti internet;
VIII aprire messaggi di posta o allegati di tipo "eseguibile", salvo il caso di *certezza* assoluta dell'identità del mittente e della sicurezza del messaggio (anche per quanto attiene virus e malware);
IX rispondere a messaggi di posta che:
1) contengono un messaggio generico di richiesta di informazioni personali per motivi non chiaramente specificati (ad es. scadenza, smarrimento, problemi tecnici) e non certamente fondati;
2) fanno uso di toni "intimidatori", quali ad esempio la minaccia del blocco della carta di credito o del conto corrente. In caso di mancata risposta dell'utente o comunque caratterizzati da elementi che possano rivelare azioni di phishing;

b) ogni singolo incaricato ha l'obbligo di:
1) limitare la dimensione dei messaggi inviati, soprattutto nei casi in cui vi siano più destinatari;
2) conservare con segretezza la password di accesso alla posta elettronica e non consentirne l'uso a terzi, modificandola secondo quanto previsto dalle istruzioni;
3) evitare ogni comportamento che possa consentire a terzi di divulgare informazioni di qualsiasi tipo riconducibili ad un mittente inconsapevole;
c) la casella di posta deve essere mantenuta in ordine, eliminando i messaggi non necessari, contenendo la dimensione degli stessi e dei relativi allegati, cancellando, pertanto, documenti inutili e soprattutto allegati ingombranti; per essa è previsto un limite massimo di MB.
d) è possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario; le comunicazioni ufficiali, in analogia a quelle da inviarsi mediante gli strumenti tradizionali, devono essere autorizzate e firmate dal Comune di Caluso e/o dai responsabili di ufficio, secondo le procedure in atto, a seconda del loro contenuto e dei destinatari delle stesse;
e) è obbligatorio porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
f) al fine di garantire l'integrale rispetto delle norme relative al corretto utilizzo della posta elettronica, il Comune di Caluso si riserva di disporre ed effettuare controlli periodici e occasionali in conformità alle norme vigenti ed al provvedimento, secondo quanto previsto nel presente disciplinare.

ANTIVIRUS E ANTIMALWARE
37. Gli strumenti elettronici sono protetti da software antivirus ed antimalware. L'incaricato deve evitare azioni volte a disabilitare o eludere il software antimalware e segnalare qualsiasi anomalia o disfunzione e deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'ente mediante virus o mediante ogni altro software aggressivo. Se riceve un qualsiasi tipo di avviso dal software antivirus o antimalware in esecuzione, l'incaricato deve seguire le istruzioni ivi indicate e, in particolare, nel caso di rilevazione di una minaccia che il software in oggetto indica come non risolvibile deve procedere a:
a) segnalare quanto sopra immediatamente al Comune di Caluso ed ai soggetti da questo indicati;
b) disconnettere il cavo di rete e, di alimentazione e nel caso di PC portatile o palmare spegnerlo;
38. È responsabilità del Comune di Caluso mantenere aggiornato il software antivirus ed antimalware, generalmente attraverso un processo automatizzato, mentre l'incaricato è connesso alle risorse di rete. È responsabilità dell'incaricato verificare il corretto funzionamento di tali software, in particolare segnalando immediatamente (attraverso apposita procedura di helpdesk) eventuali messaggi o avvisi che questi dovessero generare e/o comunque segnalando immediatamente eventuali anomalie o disfunzioni e/o particolarità (per esempio quando l'aggiornamento automatizzato non possa avvenire perché lo strumento elettronico, tipicamente PC portatili o palmari, sia utilizzato in modalità disconnessa dalla rete del Comune di Caluso).
39. L'incaricato è tenuto altresì a connettere il proprio elaboratore alla rete del Comune di Caluso, con scadenza non superiore a giorni 15, salvo motivata e certificata assenza, per consentire all'antivirus centralizzato di effettuare le scansioni di routine e controllare gli aggiornamenti.

PROTEZIONE DELLE MEMORIE DI MASSA

40. L'utente deve mantenere i dispositivi di memorizzazione e le memorie di massa, quale supporto su cui sono conservate le informazioni del Comune di Caluso ed eventuali dati, con la massima attenzione. In particolare l'incaricato deve:

a) cancellare il contenuto delle memorie non più utilizzate o da mettere a disposizione di terzi (richiedendo, se il contenuto riguarda dati sensibili, giudiziari o comunque "delicati", che la cancellazione sia effettuata dal Servizio comunale competente in maniera tecnicamente sicura ed irreversibile e comunque conforme a quanto previsto dalle norme);

b) riporre, in caso di assenza dal posto di lavoro, le eventuali memorie informatiche in dotazione, in luogo sicuro. La protezione delle stesse deve essere graduata ed ulteriormente innalzata in base alla criticità dei dati in esse contenuti.

PROTEZIONE DEI COMPUTER PORTATILI E ALTRI DISPOSITIVI MOBILI

41. Tutte le indicazioni riportate precedentemente devono essere adottate anche per i computer portatili e per gli elaboratori portatili. Per essi debbono inoltre essere adottate le seguenti ulteriori precauzioni, ponendo particolare attenzione nel caso di utilizzo dell'elaboratore in ambito esterno:

a) proteggere, se necessario, l'elaboratore portatile tramite apposito dispositivo di ancoraggio;

b) conservare in un luogo sicuro l'elaboratore portatile a fine giornata lavorativa, assicurandosi che non vi possano accedere terzi;

c) custodire con massima attenzione l'elaboratore in caso di trasporto e/o utilizzo in ambito esterno;

d) avvertire immediatamente il Comune di Caluso in caso di furto, adeguandosi alle opportune indicazioni fornite dal Comune stesso;

e) adottare, d'intesa con Comune di Caluso e nel rispetto delle procedure ed istruzioni, le misure idonee a garantire la protezione delle informazioni, anche attraverso sistemi di cifratura delle informazioni memorizzate sull'elaboratore e sistemi sicuri di accesso remoto.

È responsabilità dell'incaricato che deve operare in ambito esterno fare richiesta dei necessari strumenti di protezione.

ACCESSO Al DATI TRATTATI DAGLI UTENTI

42. Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (per esempio, aggiornamento/sostituzione/ implementazione di programmi, manutenzione hardware ecc.) o per finalità di controllo e programmazione dei costi comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Comune di Caluso, tramite il personale addetto alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, agli strumenti informatici aziendali e ai documenti ivi contenuti.

CONTROLLI E VERIFICHE

43. Per prevenire o correggere malfunzionamenti del proprio sistema nonché garantire l'efficienza dello stesso, il Comune di Caluso effettua registrazioni delle componenti di traffico (file di log) riferiti a:

a) internet: le informazioni relative ai servizi internet sono analizzate solo in forma aggregata. Alle informazioni possono accedere solo le persone interne o esterne espressamente autorizzate dal Comune di Caluso alla gestione del servizio internet.

b) rete interna: le informazioni relative ai servizi di rete interna sono raccolte, conservate ed analizzate secondo le modalità sopra descritte per il servizio internet. Ad esse possono

accedere le sole persone, interne od esterne espressamente autorizzate dal Comune di Caluso alla gestione dei servizi di rete interna;
44. Non essendo altrimenti possibile garantire l'integrale rispetto del presente disciplinare, il Comune di Caluso potrà effettuare controlli occasionali sugli strumenti elettronici, sui personal computer/elaboratori, sulle relative periferiche, sui supporti di memorizzazione e su ogni altro apparato o dispositivo elettronico.
45. In caso di anomalie, il personale incaricato effettuerà controlli anonimi che si concluderanno con avvisi generalizzati, diretti agli incaricati del settore o dell'ufficio in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti dell'ente e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
46. I controlli saranno effettuati direttamente dal Comune di Caluso, o da soggetti all'uopo espressamente autorizzati, nel rispetto delle seguenti disposizioni;
a) i controlli saranno effettuati in forma anonima, sull'intera struttura informatica comunale oppure su determinati settori, escluso il controllo mirato sul singolo incaricato. Il Comune di Caluso potrà comunicare agli incaricati, in forma anonima e collettiva, l'esito dei controlli periodici;
b) ove, in esito ad un controllo, emergano comportamenti in violazione del presente disciplinare o comunque anomali, il Comune di Caluso si riserva di effettuare, senza preavviso, una verifica finalizzata ad individuare le specifiche violazioni. In tal caso, il Comune di Caluso potrà comunicare al gruppo di incaricati sottoposti a controllo l'esito dello stesso;
e) qualora le violazioni persistessero il Comune di Caluso si riserva di procedere a controlli nei confronti di singoli incaricati e, in base alle risultanze del controllo, di avviare un procedimento disciplinare in conformità a quanto previsto dal CCNL e contratto decentrato e nel rispetto del diritto alla riservatezza dei lavoratori.
47. Per gli elementi venuti a conoscenza dal Comune di Caluso in esito o anche solo in occasione dei controlli effettuati in base al presente disciplinare valgono comunque le garanzie previste dal Dlgs 196/2003 e successive modifiche ed integrazioni.
48. Ove pervenga legittima richiesta da parte di Forze di polizia o della magistratura, le registrazioni dei file di log relativi agli incaricati interessati saranno conservate dal Comune di Caluos anche oltre i termini suddetti giorni, ai sensi dell'ari. 24 lett. f) e g) del Dlgs 196/2003, e sino che il Comune di Caluso ne abbia interesse.

DISPOSIZIONI SANZIONATOLE FINALI
49. La dotazione degli strumenti e delle risorse informatiche non costituisce in ogni caso diritto acquisito in capo al dipendente e può essere ridotta, sospesa od eliminata a discrezione del Comune di Clauos, ferma l'osservanza dell'art. 2103 cod. civ. e delle altre norme vigenti.
50. La violazione delle regole e dei divieti di cui al presente accordo comporterà,a seconda della gravita qualitativa e quantitativa e/o della eventuale reiterazione della inosservanza, l'applicazione di sanzioni disciplinari come previsto dalla normativa vigente.
51. Ad ogni fine ed effetto di legge e di CCNL il presente disciplinare e le relative disposizioni sanzionatone faranno parte a tutti gli effetti del codice disciplinare dell'ente.
52. Il contenuto del presente disciplinare costituisce anche integrazione dell'informativa fornita ai sensi dell'art. 13 del Codice D.Lgs 82/2005 e smi.
53. Le prescrizioni del presente integrano le specifiche istruzioni fornite agli incaricati in attuazione del Codice Privacy D.Lgs 196/2003.

54. Il presente disciplinare si applica a tutti gli incaricati, a tutti i dipendenti senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Comune di Caluso, a prescindere dal rapporto contrattuale con la stessa intrattenuto, ed utenti del sistema e degli strumenti suddetti (collaboratori a progetto, collaboratori coordinati, tirocinanti, stagisti ecc..).

AGGIORNAMENTO E REVISIONE

55. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente disciplinare. Le proposte verranno esaminate dal Comune di Caluso.

56. Il presente disciplinare è soggetto a verifica e revisione ogni qualvolta se ne evidenzi la necessità.

57. Il presente disciplinare sostituisce ed abroga, parzialmente o totalmente, eventuali precedenti procedure, circolari o istruzioni limitatamente alle disposizioni con esso incompatibili. Qualsiasi chiarimento al riguardo, così come sull'interpretazione ed applicazione delle disposizioni del presente potrà essere richiesta al Comune di Caluso.

58. Il disciplinare è pubblicato nella bacheca in formato elettronico all'interno di una cartella condivisa da tutti gli utenti

Allegato 6.2)

Specifiche di backup

Procedura:
i seguenti elaboratori di tipo server sono sottoposti a procedura di backup gestita da una procedura automatizzata dedicata.
Server con sistemi operativi Microsoft (MS 2k-2k3-2k8):

- SERVER.CALUSO.LOC (share - DC dominio – DHCP - Printer Server)
- SRV2003.CALUSO.LOC (share - DC dominio – DHCP - Printer Server)

Applicazione di backup e server coinvolti:

La procedura automatica è gestita dall'applicativo:
- Acronis True Image Enterprise Server - installato sul server SRV2003
- Acronis BackUp and Recovery v. 11.5 – installato su SERVER.

Supporti di backup:

i backup vengono eseguiti utilizzando il supporti del seguenti tipo:
- Nas di BackUp Synology DSM 4.2

Le sessioni di backup sono così suddivise:

Ogni giorno dal Lunedì al venerdì con partenza alle ore 21:00 viene effettuato un Backup "differenziale"

Cosa viene salvato nei backup:

La parte di S.O. e di DATI – Intero contenuto dei server.

Modalità di controllo:

A termine di ogni Backup viene mandata in automatico una mail di reportistica alla casella di posta: monitoraggio@adicomgroup.it contenente i dati di tempistica e soprattutto di esito dello stesso.
Tutte le mattine, essendo un attività che viene effettuata durante le ore serali e notturne, viene analizzato l'esito della mail di reportistica.
Viene controllato di tanto in tanto, il volume del differenziale e quando inizia a diventare consistente viene schedulato un nuovo Full, in questo modo si gestisce anche lo spazio occupato sulla NAS.

Nelle schede che seguono sono riportati esempi di back up

Da: <Acronis@comune.caluso.to.it>
A: "Adicom - Monitoraggio" <monitoraggio@adicomgroup.it>
Data invio: martedì 16 febbraio 2016 18.45
Oggetto: BCK SERVER 2008 CALUSO

1 Informazioni 16/02/2016 18.00.06 Il comando 'Esecuzione del piano di backup 'Backup " è in esecuzione.
2 Informazioni 16/02/2016 18.00.14 Il comando 'Backup' è in esecuzione.
3 Informazioni 16/02/2016 18.00.38 Analisi della partizione '1-0' in corso...
4 Informazioni 16/02/2016 18.00.40 Crea backup Differenziale
Da: Disco '1'
Al file: "file://10.48.1.182\BACKUP\server\Archivio(1)9.TIB"
Compressione: Nessuna
Escludi: File corrispondenti alla maschera
Criterio di corrispondenza: *\System Volume Information*{3808876B-C176-4e48-B7AE-04046E6CC752}; ...
Chiedi il primo supporto: No

5 Informazioni 16/02/2016 18.00.50 Operazione in sospeso 157 avviata: 'Creazione dell'immagine della partizione (System (C))'.
6 Informazioni 16/02/2016 18.01.14 Blocco della partizione 0-0 in corso...
7 Informazioni 16/02/2016 18.30.19 Operazione in sospeso 157 avviata: 'Creazione dell'immagine della partizione (ARCHIVIO (Z))'.
8 Informazioni 16/02/2016 18.44.49 Operazione in sospeso 154 avviata: 'Salvataggio della struttura della partizione (Disco rigido 1)'.
9 Informazioni 16/02/2016 18.44.57 Il comando 'Backup' è stato completato correttamente.
Attività 'Backup differenziale' completata sulla macchina 'server.caluso.loc'.

--

Da: "Adicom - Monitoraggio" <monitoraggio@adicomgroup.it>
A: "Adicom - Monitoraggio" <monitoraggio@adicomgroup.it>
Data invio: martedì 16 febbraio 2016 22.14
Oggetto: Acronis True Image Notification from srv2003.caluso.loc

1 Information 16/02/2016 22:00 The "bck" operation started
2 Information 16/02/2016 22:00 Analyzing partition 0-0...
3 Information 16/02/2016 22:00 Analyzing partition C:...
4 Information 16/02/2016 22:00 Analyzing partition 0-0...
5 Information 16/02/2016 22:00 Analyzing partition F:...
6 Information 16/02/2016 22:00 Analyzing partition C:...
7 Information 16/02/2016 22:00 Analyzing partition F:...
8 Information 16/02/2016 22:00 Create Differential Backup ArchiveFrom: Disk 1, Disk 2To file: "\\10.48.1.182\backup\srv2003\srv2k3.tib"Compression: High
9 Information 16/02/2016 22:00 Pending operation 126 started: "Saving partition structure"
10 Information 16/02/2016 22:00 Pending operation 129 started: "Creating partition image"
11 Information 16/02/2016 22:00 Locking partition C:...
12 Information 16/02/2016 22:03 Pending operation 126 started: "Saving partition structure"
13 Information 16/02/2016 22:03 Pending operation 129 started: "Creating partition image"
14 Information 16/02/2016 22:14 Operation has succeeded.

Allegato 6.3)

Studio di fattibilità tecnica relativo al piano di continuità operativa e disaster recovery

Il Comune di Caluso sta approvando lo studio di fattibilità tecnica per la Continuità Operativa ed il Disaster Recovery, la relativa deliberazione di approvazione della Giunta Comunale diverrà parte integrante del presente allegato.