Ministero dell'Istruzione, dell'Università e della Ricerca

ISTITUTO COMPRENSIVO ñMARGHERITA HACKò MANIAGO

Allegati al

Manuale di Gestione

Del Protocollo Informatico

-

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Sono escluse dalla protocollazione, ai sensi dellôart. 53. c. 5 del DPR n. 445/2000 le seguenti tipologie documentarie:

- Gazzette ufficiali, Bollettini ufficiali PA
- Notiziari PA
- Giornali, Riviste, Libri
- Materiali pubblicitari
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte o preventivi di terzi non richiesti
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti dôoccasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni)
- convocazioni ad incontri o riunioni e corsi di formazione interni
- delibere, disposizioni interne, ordini di servizio e comunicazioni al personale
- modulistica attinente a ferie, missioni, fornitura di materiali ed equipaggiamenti informatici, rapporti valutativi e documentazione simile
- atti notificati a mano ai dipendenti
- ricevute di ritorno delle raccomandate A.R

REGOLE DI RACCOLTA E CONSEGNA DELLA CORRISPONDENZA CONVENZIONALE AL SERVIZIO POSTALE NAZIONALE

1. La corrispondenza viene raccolta periodicamente (ogni Lunedì e Giovedì) dal servizio postale pubblico dal personale dellôUfficio Posta della UOP dellôAmministrazione/AOO;
2. La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, viene consegnata in busta chiusa al servizio postale pubblico in occasione della raccolta periodica della corrispondenza;

ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto allôinterno dellôAmministrazione/AOO un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati.
Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche lôanno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette allôaccesso ordinariamente previsto

16.17.1 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE PER TUTTE LE AMMINISTRAZIONI

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dellôattività amministrativa;
- I documenti anonimi individuati ai sensi dellôart. 8, comma 4, e 141 del codice di procedura penale;
- corrispondenza legata a vicende di persone o a fatti privati o particolari;
- le tipologie di documenti individuati dallôart. 24 della legge 7 agosto 1990 n. 241, dallôart. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

MODULO DI CONSULTAZIONE DELLA SEZIONE DI DEPOSITO E STORICA DELLôARCHIVIO

Spett.le Dirigente Scolastico
IC MANIAGO

Oggetto: Richiesta di consultazione del materiale documentario conservato nella sezione di deposito/storica dellôArchivio generale dellôAmministrazione.

Scopo della consultazione:
.....
.....
Durata indicativa della consultazione: ..... mesi

Materiale da consultare:
- **Titolo** .....
- **Classe** .....
- **Sottoclasse** .....

o **Descrizione dei fascicoli:**

- Oggetto del fascicolo: .....
- Anno di repertoriazione .....
- Dal numero ..... al numero .....

o **Descrizione dei sottofascicoli:**

- Oggetto del fascicolo: .....
- Anno di repertoriazione .....
- Dal numero ..... al numero .....

NOTE:

.....

.....

lì .....

LôOPERATORE RICEVENTE: .....

IL RESPONSABILE DELLôARCHIVIO: .....

POLITICHE DI SICUREZZA

POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATICO

1.1 Premessa

1. Lôincarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere lôAmministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dallôAmministrazione in termini di apertura, fiducia e integrità del sistema informativo.

2. Sono di proprietà dellôAmministrazione i sistemi di accesso ad Internet, lôIntranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nellôinteresse dellôAmministrazione e in rapporto con possibili interlocutori della medesima.

3. Lôefficacia e lôefficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dellôAmministrazione ed i loro interlocutori che vivono con lôinformazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

1.2 Scopo

1. Lo scopo di queste politiche è sottolineare lôuso accettabile del sistema informatico dellôAmministrazione.

2. Le regole sono illustrate per proteggere gli impiegati e lôAmministrazione.

3. Lôuso non appropriato delle risorse strumentali espone lôAmministrazione 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.

1.3 Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dellôAmministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati della/e ditta/e < *inserire nome* > , includendo tutto il personale affiliato con terze parti.

2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dellôAmministrazione o ñaffittateò da questa.

1.4 Politiche ï Uso generale e proprietà

1. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dellôAmministrazione e comunque trattati, rimangono di proprietà della medesima.

2. Gli impiegati sono responsabili dellôuso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dellôinformazione memorizzata su ciascun componente òpersonaleò della rete dato che lôamministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.

3. Le singole aree o settori o Divisioni o Direzioni, sono responsabili della creazione di linee guida per lôuso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dellôAmministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente.

4. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dallôAmministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

5. Per i motivi di cui sopra lôAmministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

1.5 Politiche Sicurezza e proprietà dellôinformazione

1. Il personale dellôAmministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.

2. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dellôuso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.

3. Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso lôattivazione automatica del salva schermo protetto da password o la messa in *stand-by* con un comando specifico.

4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dallôAmministrazione.

5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.

6. Eventuali attività di scambio di opinioni del personale dellôAmministrazione allôinterno di ñnew groupò che utilizzano il sistema di posta elettronica dellôAmministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dellôAmministrazione a meno che non si tratti di discussioni inerenti e di interesse dellôAmministrazione eseguite per conto della medesima.

7. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dellôAmministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dellôAmministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dellôAmministrazione ed aggiornato.

8. Il personale deve usare la massima attenzione nellôapertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.

9. Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

2 POLITICHE ANTIVIRUS

2.1 Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.

I danni causati dai virus allôAmministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.

I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

2.2 Scopo

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dellôAmministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

2.3 Ambito di applicazione

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dellôAmministrazione è tenuto a rispettare le politiche di seguito richiamate.

2.4 Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dellôAmministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata

con la più recente versione resa disponibile sul sito centralizzato.

ÅNon aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.

ÅNon aprire mai messaggi ricevuti in risposta a messaggi ñprobabilmenteò mai inviati.

Å Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.

ÅNon scaricare mai messaggi da siti o sorgenti sospette.

Å Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dellôamministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.

Å Evitare lôuso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.

ÅEvitare lôutilizzo, non controllato, di uno stesso computer da parte di più persone.

ÅEvitare collegamenti diretti ad Internet via modem.

ÅNon utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.

Å Se si utilizza una postazione di lavoro che necessita di un ñbootstrapò da supporti di archiviazione rimovibili, usare questo protetto in scrittura.

ÅNon utilizzare i server di rete come stazioni di lavoro.

Å Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.

Å Effettuare una scansione della postazione di lavoro con lôantivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dellôOrganizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dellôAmministrazione ed, eventualmente, allôesterno.

Å Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dellôAmministrazione, siano dotati di adeguate misure di protezione antivirus.

ÅIl personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.

Å I supporti di archiviazione rimovibili provenienti dallôesterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).

Å Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dallôArticolo 615 quinquies del Codice penale concernente la ñDiffusione di programmi diretti a danneggiare o interrompere un sistema informaticoé [omissis]é che prevede la reclusione sino a due anni e la multa sino a lire venti milioniò.

ÅIl software acquisito deve essere sempre controllato contro i virus e verificato perché

sia di uso sicuro prima che sia installato.

- È proibito lôuso di qualsiasi software diverso da quello fornito dallôAmministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dellôevoluzione delle tecnologie disponibili sul mercato.

2.5 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare lôevento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare lôantivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare lôAntivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
- diffondere la notizia dellôevento, allôinterno dellôAmministrazione, nelle forme opportune.

3 POLITICHE USO NON ACCETTABILE

1. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto allôinterno dellôAmministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).
2. In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dellôAmministrazione.
3. Lôelenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, lôinstallazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dallôAmministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto dôautore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale lôAmministrazione o lôutente finale non ha una licenza attiva.
3. È rigorosamente proibita lôesportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dellôAmministrazione.

5. Rivelazione delle credenziali personali ad altri o permettere ad altri lôuso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro dôufficio è fatto da casa o a casa.
6. Usare un sistema dellôAmministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dellôAmministrazione con lôaggravante dellôuso di credenziali fornite dallôAmministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nellôambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dellôAmministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
   a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
   b. attività di ñsniffingò;
   c. disturbo della trasmissione;
   d. spoofing dei pacchetti;
   e. negazione del servizio;
   f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
   g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare lôaccesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dellôAmministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne allôAmministrazione.

3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo ñmessaggi spazzaturaò, o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con lôintento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per

pubblicizzare servizi erogati dallôAmministrazione e fruibili via Intranet stessa.

6. Invio di messaggi non legati alla missione dellôAmministrazione ad un grande numero di destinatari utenti di news group (news group spam).

4 LINEE TELEFONICHE COMMUTATE (ANALOGICHE E DIGITALI)

4.1 Scopo

1. Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).
2. Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dellôAmministrazione.

4.2 Ambito di applicazione

1. Queste politiche sono relative solo a quelle linee che sono terminate allôinterno della/e sede/i dellôAmministrazione. Sono pertanto escluse le eventuali linee collegate con le abitazioni degli impiegati che operano da casa e le linee usate per gestire situazioni di emergenza.

4.3 Politiche ï Scenari di impatto sullôAmministrazione

1. Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.
2. Il *primo* è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.
3. Il *secondo* scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dellôAmministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso lôintruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dellôAmministrazione attraverso la rete locale e, dallôaltro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dellôAmministrazione, comprese quelle vitali.

4.4 Politiche ï Collegamento di PC alle linee telefoniche analogiche

1. La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.

2. Le linee commutate rappresentano una significativa minaccia per lôAmministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

4.5 Politiche ï Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dellôincaricato allôuso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

Å una chiara e dettagliata relazione che illustri la necessità di una linea commutata

dedicata in alternativa alla disponibilità di rete sicura dellôAmministrazione;

- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e lôhardware che deve essere collegato alla linea e utilizzato dallôincaricato;
- che cosa la connessione esterna richiede per essere acceduta.

5 POLITICHE PER LôINOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

5.1 Scopo

1. Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dellôAmministrazione

5.2 Ambito di applicazione

1. Queste politiche riguardano lôinoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

5.3 Politiche

1. Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio allôesterno dellôAmministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati allôesterno dellôAmministrazione.
2. Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

6 POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE COMMUTATA

6.1 Scopo

1. Proteggere le informazioni elettroniche dellôAmministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dallôesterno su rete commutata.

6.2 Ambito di applicazione

1. Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

6.3 Politiche

1. Il personale dellôAmministrazione e le persone terze autorizzate (clienti, venditori, altre amministrazioni, cittadini, etc.) possono utilizzare la linea commutata per guadagnare lôingresso alla Intranet dellôAmministrazione. Tale accesso dovrebbe essere rigidamente controllato usando sistemi di autenticazione forte, quali: password da usare una sola volta (one time password), sistemi di firma digitale o tecniche di sfida/risposta (challenger/response).
2. È responsabilità del personale con i privilegi di accesso dallôesterno alla rete dellôAmministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dellôAmministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dellôAmministrazione dallôesterno deve essere consapevole che tale accesso costituisce ñrealmenteò una estensione del

sistema informativo che potenzialmente può trasferire informazioni sensitive.

3. Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dellôAmministrazione.
4. Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reinstradamento della connessione.

7 POLITICHE PER LôUSO DELLA POSTA ISTITUZIONALE DELLôAMMINISTRAZIONE

7.1 Scopo

1. Evitare lôoffuscamento dellôimmagine dellôAmministrazione. Quando un messaggio di posta esce dallôAmministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dellôAmministrazione.

7.2 Ambito di applicazione

1. La politica di seguito descritta intende illustrare lôuso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dellôAmministrazione stessa.

7.3 Politiche ï Usi proibiti

1. Il sistema di posta dellôAmministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

7.4 Politiche ï Uso personale

1. È considerato accettabile lôuso personale della posta istituzionale dellôAmministrazione a condizione che:
   - Åi messaggi personali siano archiviati in cartelle separate da quelle di lavoro;
   - Åvenga utilizzata una ragionevole quantità di risorse pubbliche;
   - Ånon si avviino catene di lettere o messaggi scherzosi, di disturbo o di altro genere.
2. Il personale dellôAmministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.
3. LôAmministrazione può però controllare senza preavviso i messaggi che transitano in rete per verificare il rispetto delle politiche concernenti gli ñusi proibitiò di cui sopra.
4. Non è ammesso lôuso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

8 POLITICHE PER LE COMUNICAZIONI WIRELESS

8.1 Scopo

1. Queste politiche proibiscono lôaccesso alla rete dellôAmministrazione via rete wireless insicura.

2. Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti allôAmministrazione.

8.2 Ambito di applicazione

1. La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dellôAmministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere ñpacchettiò di dati.
2. Dispositivi wireless e/o reti senza connettività alla Intranet dellôAmministrazione, sono esclusi da queste politiche.

8.3 Politiche ï Registrazione delle schede di accesso

1. Tutti i ñpunti di accessoò o le ñstazioni baseò collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. Questi dispositivi sono soggetti a periodiche ñprove di penetrazioneò e controlli (auditing). Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

8.4 Politiche ï Approvazione delle tecnologie

1. Tutti i dispositivi di accesso alle LAN dellôAmministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

PIANO FORMATIVO PER IL PERSONALE

Amministrazione IC MANIAGO

Tenute presenti le disponibilità di bilancio, in relazione anche al combinato disposto dellôart. 2 del CCNL 31 marzo 1999 e dellôart. 4 del CCNL 1 aprile 1999, nella impossibilità di organizzare autonomi corsi, è favorita lôadesione a corsi di formazione gratuiti organizzati, per il personale impegnato nelle attività di registrazione del protocollo, dalle amministrazioni centrali o territoriali.

NORMATIVA DI RIFERIMENTO

1. *Legge 7 agosto 1990*, n. 241 Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. del 18 agosto 1990, n. 192)
2. *DPR 27 giugno 1992*, n. 352 Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dellôart. 24, comma 2, della Legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. 29 luglio 1992, n. 177)
3. *DPR 12 febbraio 1993*, n. 39 Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dellôart. 2, comma 1, lettera m), della legge 23 ottobre 1992, n. 421. (G.U. 10 febbraio 1993, n. 42)
4. *Legge 15 marzo 1997*, n. 59 Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa.
5. *DPCM 28 ottobre 1999* Gestione informatica dei flussi documentali nelle pubbliche amministrazioni. (G.U. 11 dicembre 1999, n. 290)
6. *Decreto legislativo 29 ottobre 1999*, n. 490 Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dellôarticolo 1 della legge 8 ottobre 1997, n. 352. (G.U. 27 dicembre 1999, n. 302)
7. *DPCM 31 ottobre 2000* Regole tecniche per il protocollo informatico; valido ai sensi dellôart. 78 del DPR 28 dicembre 2000, n. 445. (G.U. n. 272 del 21 novembre 2000)
8. *Deliberazione AIPA 23 novembre 2000*, n. 51Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dellôart. 18, comma 3, del DPR 10 novembre 1997, n. 513. (G.U. 14 dicembre 2000, n. 291)
9. *DPR 28 dicembre 2000*, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42)
10. *Circolare del 16 febbraio 2001*, n. AIPA/CR/27 ï ñArt. 17 del DPR 10 novembre 1997, n. 513 Utilizzo della firma digitale nelle pubbliche amministrazioniò.
11. *Decreto legislativo 30 marzo 2001*, n. 165 ñNorme generali sullôordinamento del lavoro alle dipendenze delle amministrazioni pubblicheò.
12. *Circolare AIPA 7 maggio 2001*, n. AIPA/CR/28 Articolo 18, comma 2, del DPCM 31 ottobre 2000 recante regole tecniche per il protocollo informatico di cui al DPR 28 dicembre 2000, n. 445 Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati. (G.U. 21 novembre 2000, n. 272)
13. *Circolare AIPA 21 giugno 2001*, n. AIPA/CR/31 (Art. 7, comma 6, del DPCM 31 ottobre 2000 recante ñRegole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428ò requisiti minimi di sicurezza dei sistemi operativi disponibili.)
14. *Direttiva del Ministro per la funzione pubblica del 13 dicembre 2001* Formazione del personale. (G.U. del 31 gennaio 2002, n. 26)
15. *Direttiva 16 gennaio 2002*, Dipartimento per lôinnovazione e le tecnologie Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali.
16. *Decreto legislativo 23 gennaio 2002*, n. 10 Recepimento della direttiva 1999/93/CE sulla firma elettronica.
17. *Direttiva del Ministro per lôinnovazione e le tecnologie, 9 dicembre 2002* -Trasparenza

dellôazione amministrativa e gestione elettronica dei flussi documentali.

18. *Direttiva del Ministro per lôinnovazione e le tecnologie, 20 dicembre* 2002 Linee guida in materia di digitalizzazione dellôamministrazione.
19. *Legge 27 dicembre 2002*, n. 289 Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
20. *DPR 7 aprile 2003*, n. 137 Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dellôarticolo 13 del decreto legislativo 23 gennaio 2002.
21. *Decreto legislativo 30 giugno 2003*, n. 196 Codice in materia di protezione dei dati personali.
22. *Decreto Ministeriale 14 ottobre 2003* Approvazione delle linee guida per lôadozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249)
23. *Direttiva del Ministro per lôinnovazione e le tecnologie 27 novembre* 2003 Impiego della posta elettronica nelle pubbliche amministrazioni. (G.U. 12 gennaio 2004, n. 8)
24. *Direttiva 1999/93/CE del Parlamento europeo e del consiglio del 13 dicembre 2003.*
25. *Direttiva 18 dicembre 2003* Linee guida in materia di digitalizzazione dellôamministrazione per lôanno 2004. (G.U. 4 aprile 2004, n. 28)
26. *DPCM 13 gennaio 2004* Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (G.U. 27 aprile 2004, n. 98)
27. *Deliberazione CNIPA 19 febbraio 2004*, n. 11 Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.
28. *Decreto legislativo 22 gennaio 2004*, n. 42 Codice dei beni culturali e del paesaggio, ai sensi dellôart. 10 della legge 6 luglio 2002, n. 137. (G.U. 24 febbraio 2004, n. 28).
29. *L. 28 gennaio 2009, n. 2* Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale (estratto relativo alla PEC)

29. *DPCM 30 marzo 2009* Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
30. *L. 18 giugno 2009, n. 69* Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile (estratto relativo allôAmministrazione digitale)

29. *DECRETO LEGISLATIVO 30 dicembre 2010*, n. 235 Modifiche ed integrazioni al decreto legislativo 7 Marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69. (11G0002) (GU n.6 del 10-1-2011 - Suppl. Ordinario n. 8)
30. *DPCM 22 luglio 2011* Comunicazioni Imprese PA
31. *Circolare AGID del 23 gennaio 2013, n 60* Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni.
32. *Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013* - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario;

32. *Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013* - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione

digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario;

33. *Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014* - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 8 del 12 gennaio 2015;

ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE

NOMINATIVO	TITOLO/RUOLO NELLôAOO	ESTREMI E DESCRIZIONE DELLA DELEGA RICEVUTA
Dott.ssa Livia Cappella	Dirigente	
Dott.ssa Mara Bonitta	Direttore SS.GG.AA.	