

## NR. 142 DEL REGISTRO DELLE DELIBERAZIONI

### VERBALE DI DELIBERAZIONE DELLA GIUNTA MUNICIPALE

**OGGETTO: APPROVAZIONE MANUALE DI GESTIONE DEL  
PROTOCOLLO INFORMATICO, DEI FLUSSE  
DOCUMENTALI E DEGLI ARCHIVI COMUNALI.**

L' anno DUEMILAQUINDICI addì SEDICI del mese di OTTOBRE , alle ore 11,50 ,  
nella Sede Municipale.

Previa notifica degli inviti personali, avvenuta nei modi e termini di legge, si e' riunita  
la Giunta Comunale.

NR.	COGNOME E NOME	CARICA	P	A
01	SERO Filippo Giovanni	Sindaco		A
02	MONTESANTO Leonardo	Assessore	P	
03	CELESTE Leonardo	Assessore	P	
04	DONNICI Giuseppe	Assessore	P	
05	RIZZO Cataldo	Assessore	P	

TOTALE PRESENTI : 04

TOTALE ASSENTI : 01

ASSISTE il Segretario : DOTT. SSA CLAUDIA DONATO  
Il Sig. Leonardo MONTESANTO nella qualità di SINDACO F.F. assunta la presidenza  
e constatata la legalità della adunanza dichiara aperta la seduta e pone in discussione  
la seguente pratica segnata all' ordine del giorno.

%%%

## LA GIUNTA COMUNALE

**Richiamato** - il proprio "Regolamento per la tenuta del protocollo e dell'archivio - manuale per la gestione del protocollo informatico" approvato con deliberazione di giunta comunale n. 27 del 26.02.2004;

**VISTA** la deliberazione di Giunta Municipale n. 141 del 16/10/2015 ad oggetto : Individuazione Della AOO e Nomina del Responsabile della Gestione Informatica, dei Flussi Documentali e Degli Archivi ;

**CHE** con l'uscita delle regole tecniche contenute nel DPCM del 03 dicembre 2013 e pubblicate nella G.U. del 12 marzo 2014 gli Enti sono chiamati ad aggiornarlo secondo le indicazioni stabilite dalla normativa;

**Premesso che :**

- Il D.P.R. 445/2000 "Disposizioni legislative in materia di documentazione amministrativa" prevede, nella sezione III denominata tenuta e conservazione del sistema di gestione dei documenti, l'articolo 61 secondo il quale ogni amministrazione provvede ad istituire un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi posto alla dirette dipendenze di un dirigente ovvero un funzionario in possesso di idonei requisiti professionali o di professionalità tecnica;

- Il D.P.C.M. 3/12/2013 "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" disciplina all'articolo 5 il manuale di gestione che descrive il sistema di gestione e di conservazione dei documenti fornendo le istruzioni per il corretto funzionamento del servizio e per la tenuta del protocollo informatico;

**Preso atto che :**

- il manuale di gestione nel recepire le norme in materia di formazione, gestione, archiviazione, conservazione dei documenti informatici del comune, disciplina il servizio di protocollo informatico, di gestione e conservazione documentale, la spedizione di documenti, la gestione dei flussi documentali interni, i fascicoli informatici, la sicurezza dati, delle tecnologie e della infrastruttura di rete;

**Dato atto che :**

- l'articolo 5 del D.P.C.M. 3-12-2013 "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" stabilisce che l'Amministrazione adotta il presente Manuale di Gestione su proposta del Responsabile del Servizio precisando altresì che gli eventuali aggiornamenti del Manuale sono parimenti predisposti dallo stesso per la sottoposizione della nuova stesura agli organi competenti per l'approvazione;

- Il Manuale deve essere pubblicato sul sito informatico istituzionale dell'ente;

**Valutate**

- Le linee guida DIGIT PA ora AGID per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi;

**Richiamate :**

- La legge 241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";

- la legge 150/2000 "Disciplina delle attività di informazione e comunicazione delle Pubbliche Amministrazioni";

- Il D.P.R. 445/2000 "Disposizioni legislative in materia di documentazione amministrativa";

- Il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali";
- Il D.P.R. 68/2005 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3";
- La deliberazione Cnipa (ora Agid) 11/2004 "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali";
- Il D.Lgs. 82/2005 "Codice dell'amministrazione digitale";
- il D.P.C.M. 3/12/2013 "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";

**Ritenuto** opportuno procedere all'approvazione di un nuovo manuale di gestione che tenga conto delle nuove disposizioni scaturite dalla necessità di usare strumenti tecnologici all'avanguardia;

**Attesa** la propria competenza ai sensi dell'art. 48 del D. Lgs. 18/08/2000, n. 267 - T.U. Enti Locali;

**Visti** i pareri previsti dall'ex art. 49 e 147/bis del T.U. n. 267/00 e s.m.i., che si allegano alla presente atto per farne parte integrante e sostanziale;

**Visto** il testo unico delle leggi sull'Ordinamento degli enti locali approvato con decreto legislativo 18 agosto 2000, n. 267;

**A voti** unanimi favorevoli espressi nelle forme di legge,

## D E L I B E R A

La premessa narrativa è parte integrante e sostanziale del presente dispositivo;

- 1) di approvare il "Manuale di Gestione del Protocollo Informatico, dei flussi documentali e degli archivi comunali", che costituisce parte integrante e sostanziale del presente (Allegato 1);
- 2) di stabilire che il presente manuale di gestione entra in vigore dalla data di pubblicazione del presente dispositivo;
- 3) Revocare parzialmente la deliberazione di G.M. n. 27 del 26.02.2004 nella parte relativa al manuale per la gestione del protocollo informatico;
- 4) di pubblicare il Manuale con gli allegati sul sito informatico istituzionale del Comune;
- 5) Con separata ed unanime votazione si dichiara immediatamente eseguibile la presente deliberazione, ai sensi dell'art. 134 - 4° comma - del Decreto Legislativo 18/08/2000 n. 267.



**COMUNE DI CARIATI**  
(Prov. di COSENZA)

**MANUALE DI GESTIONE  
DEL PROTOCOLLO INFORMATICO,  
DEI FLUSSI DOCUMENTALI  
E DEGLI ARCHIVI COMUNALI**

(Regolamento adottato ai sensi dell'art. 5 del D.P.C.M. 3/12/2013,  
Gazzetta Ufficiale n. 59 del 12 marzo 2014)

Adottato con Delibera di Giunta Municipale

n. \_142 del 16 ottobre 2015

*fr*

## Sommario

I – PRINCIPI GENERALI.....	6
Art. 1: Oggetto .....	6
Art. 2: Definizioni .....	6
Art. 3: Area Organizzativa Omogenea (AOO).....	6
Art. 4: Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi	7
Art. 5: Conservazione delle copie del registro informatico di protocollo.....	8
Art. 6: Firma digitale qualificata. Abilitazione dei dipendenti .....	8
Art. 7: Caselle di Posta elettronica.....	8
Art. 8: Sistema di classificazione dei documenti.....	8
II – PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO .....	9
Art. 9: Protocolli diversi dal protocollo informatico .....	9
III – PIANO PER LA SICUREZZA INFORMATICA .....	9
Art. 10: Piano per la sicurezza informatica .....	9
Art. 11: Politiche di sicurezza .....	9
IV – MODALITA' DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DI DOCUMENTI.....	12
Art. 12: Principi generali .....	12
Art. 13: Documento ricevuto dall'Amministrazione .....	13
Art. 14: Documento inviato dall'Amministrazione .....	13
Art. 15: Documento interno formale .....	14
Art. 16: Documento interno informale.....	14
V – DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI .....	14
Art. 17: Ricezione di documenti informatici sulla casella di posta istituzionale.....	14
Art. 18: Ricezione di documenti informatici su supporti rimovibili .....	14
Art. 19: Ricezione di documenti cartacei a mezzo posta convenzionale.....	15
Art. 20: Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali .....	15
Art. 21: Errata ricezione di documenti digitali.....	15
Art. 22: Errata ricezione di documenti cartacei.....	15
Art. 23: Rilascio di ricevute attestanti la ricezione di documenti informatici .....	15
Art. 24: Rilascio di ricevute attestanti la ricezione di documenti cartacei .....	16
Art. 25: Archiviazione dei documenti informatici.....	16
Art. 26: Classificazione, assegnazione, fascicolazione e presa in carico dei documenti.....	16
Art. 27: Verifica formale dei documenti da spedire .....	16

Art. 28: RegISTRAZIONI di protocollo e segnatura dei documenti in partenza e interni .....	17
Art. 29: Trasmissione di documenti informatici .....	17
Art. 30: Spedizione di documenti cartacei a mezzo posta .....	17
Art. 31: Ricezione e trasmissione di documenti cartacei a mezzo telefax.....	17
Art. 32: Ricevute di trasmissione .....	18
VI – REGOLE DI ASSEGNAZIONE E SMISTAMENTO DEI DOCUMENTI RICEVUTI .....	18
Art. 33: Regole generali .....	18
Art. 34: Assegnazione e smistamento di documenti ricevuti in formato digitale .....	18
Art. 35: Assegnazione e smistamento di documenti ricevuti in formato cartaceo .....	19
VII – U.O. RESPONSABILI DELLE ATTIVITA' DI REGISTRAZIONI DI PROTOCOLLO, DI ORGANIZZAZIONE E TENUTA DEI DOCUMENTI .....	19
Art. 36: Ufficio Protocollo e Archivio comunale .....	19
Art. 37: Servizio per la conservazione elettronica dei documenti .....	20
VIII – DOCUMENTI ESCLUSI DALLA REGISTRAZIONE O SOGGETTI A REGISTRAZIONE PARTICOLARE.....	20
Art. 38: Documenti esclusi dalla registrazione di protocollo.....	20
Art. 39: Documenti soggetti a registrazione particolare .....	20
IX – SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE.....	21
Art. 40: Generalità .....	21
Art. 41: Piano di conservazione .....	22
Art. 42: Titolare di classificazione .....	22
Art. 43: Fascicolazione dei documenti .....	41
Art. 44: Apertura e chiusura del fascicolo.....	41
Art. 45: Modifica delle assegnazioni dei documenti ai fascicoli .....	42
Art. 46: Repertorio dei fascicoli .....	42
Art. 47: Serie archivistiche e relativi repertori.....	42
Art. 48: Versamento dei documenti nell'archivio di deposito.....	43
Art. 49: Verifica dei documenti riversati nell'archivio di deposito .....	43
Art. 50: Scarto archivistico .....	43
Art. 51: Consultazione degli archivi .....	43
X – MODALITA' DI PRODUZIONE E CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO .....	44
Art. 52: Unicità del protocollo informatico.....	44
Art. 53: Registro giornaliero di protocollo .....	44
Art. 54: RegISTRAZIONI di protocollo .....	44
Art. 55: Elementi facoltativi delle regISTRAZIONI di protocollo.....	45
Art. 56: Segnatura di protocollo dei documenti .....	45

SB

Art. 57: Annullamento delle registrazioni di protocollo .....	46
Art. 58: Documenti con più destinatari .....	46
Art. 59: Protocollazione di telegrammi.....	46
Art. 60: Protocollazione di telefax .....	46
Art. 61: Protocollazione di corrispondenza digitale già pervenute cartacea.....	47
Art. 62: Protocollazione di un numero consistente di documenti.....	47
Art. 63: Corrispondenza relativa alle gare d'appalto .....	47
Art. 64: Corrispondenza pervenuta per posta raccomandata .....	47
Art. 65: Protocolli urgenti .....	47
Art. 66: Documenti anonimi o non firmati .....	47
Art. 67: Corrispondenza personale o riservata .....	48
Art. 68: Corrispondenza consegnata con ricevuta .....	48
Art. 69: Integrazioni documentarie.....	48
XI – DESCRIZIONE FUNZIONALE ED OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO .....	48
Art. 70: Descrizione del sistema di protocollo informatico .....	48
XII – RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI.....	48
Art. 71: Generalità .....	48
Art. 72: Profili di accesso.....	49
Art. 73 : Rete delle comunicazioni di avvenuta protocollazione.....	49
XIII – MODALITA' DI UTILIZZO DEL REGISTRO DI EMERGENZA.....	49
Art. 74: Registro di emergenza .....	49
Art. 75: Apertura del registro di emergenza.....	49
Art. 76: Utilizzo del registro di emergenza .....	50
Art. 77: Chiusura e recupero del registro di emergenza.....	50
XIV - NORME GENERALI PER LA PRESENTAZIONE DI PRATICHE DE-MATERIALIZZATE .....	50
Art. 78 – Definizioni .....	50
Art. 79 – Modalità di invio telematico .....	51
Art. 80 - Procedure d'emergenza.....	52
Art. 81 - Oggetto del messaggio di posta elettronica .....	52
Art. 82- Invii multipli e successivi.....	52
Art. 83 – Arrivi multipli e successivi .....	52
Art. 84 - Pratiche inviate su supporto cartaceo .....	53
Art. 85 - Bolli, imposte e diritti.....	53
XV – NORME TRANSITORIE E FINALI.....	53
Art. 86: Norma transitoria relativa alla irretroattività del titolare .....	53

sh

Art. 87: Pubblicità del presente manuale .....	53
Art. 88: Entrata in vigore.....	53
Allegato "A" .....	54
Definizioni .....	54
ALLEGATO "B" .....	60
Descrizione funzionale ed operativa del sistema di protocollo informatico .....	60



## I – PRINCIPI GENERALI

### Art. 1: Oggetto

1. Il presente Manuale di Gestione, adottato ai sensi della normativa vigente<sup>1</sup>, disciplina le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici, in relazione ai procedimenti amministrativi del **Comune di CARIATI**

### Art. 2: Definizioni

1. Ai fini del presente manuale di gestione si intende per:

- a) "AMMINISTRAZIONE", il **Comune di CARIATI**;
  - b) "TESTO UNICO", il D.P.R. 20.12.2000, n. 445 recante "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
  - c) "C.A.D.", il D. Lgs. 7/03/2005, n. 82 recante "Codice dell'amministrazione digitale";
  - d) "REGOLE TECNICHE PI", il D.P.C.M. 3.12.2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del C.A.D.";
  - d-bis) "REGOLE TECNICHE CONS", D.P.C.M. 3.12.2013 "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"
  - e) "AOO", l'Area Organizzativa Omogenea;
  - f) "RPA", il Responsabile del Procedimento Amministrativo;
  - g) "RSP", il Responsabile per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
  - h) "UOP", l'Unità Organizzativa di registrazione di Protocollo, cioè l'ufficio che svolge attività di registrazione di protocollo;
  - i) "UU", l'Ufficio Utente, cioè l'ufficio destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali; in linea di massima ogni UU corrisponde ad un Servizio dell'Amministrazione.
2. Per le altre definizioni si rimanda all'Allegato "A" del presente Manuale di gestione.

### Art. 3: Area Organizzativa Omogenea (AOO)

1. Individuare l'A.O.O. già denominata sull'IPA (Indice delle Pubbliche Amministrazioni) Area Segreteria Affari Generali quale unica Area Organizzativa Omogenea (AOO) nell'ambito dell'Amministrazione Comunale di Cariatì per la gestione dei documenti e dei flussi documentali ai sensi dell'articolo 50 comma 4 del dpr 28 dicembre 2000, n. 445.

---

<sup>1</sup> Art. 5 delle "REGOLE TECNICHE"

a) i dati identificativi dell'Amministrazione

Codice identificativo dell'Amministrazione	<b>c_b774</b>
Nome esteso dell'Amministrazione	<b>COMUNE DI CARIATI</b>
Indirizzo della sede principale dell'AOO a cui indirizzare la corrispondenza convenzionale	<b>COMUNE DI CARIATI PIAZZA ROCCO TRENTO 87062 CARIATI (CS)</b>
Nome referente :	<b>CATALDO</b>
Cognome referente :	<b>RUSSO</b>

b) i dati identificativi dell' AOO individuata

Codice identificativo dell'AOO	<b>AOO_02</b>
Nome esteso dell'AOO	<b>AREA SEGRETERIA AFFARI GENERALI</b>
Indirizzo di posta elettronica certificata istituzionale :	<b>comune.cariati@asmepec.it</b>
Nome del Responsabile:	<b>CATALDO</b>
Cognome del Responsabile:	<b>RUSSO</b>
Data istituzione	<b>07/11/2012</b>
Numero "n" uffici afferenti	<b>01</b>

c) i dati identificativi del Servizio attivato AOO

Codice ufficio	
Denominazione	<b>SERVIZIO PROTOCOLLO GENERALE</b>
Codice dell'AOO di appartenenza	<b>AREA SEGRETERIA AFFARI GENERALI</b>
Nome del Responsabile Servizio di Protocollo Informatico della gestione documentale	<b>CATALDO</b>
Cognome del Responsabile Servizio di Protocollo Informatico della gestione documentale	<b>RUSSO</b>
Nome del vicario del Responsabile Servizio di Protocollo Informatico della gestione documentale	<b>PASQUALE</b>
Cognome del vicario Responsabile	<b>LE PERA</b>
Nome del vicario del Responsabile Servizio di Protocollo Informatico della gestione documentale	<b>BENEDETTO</b>
Cognome del vicario Responsabile	<b>MUSSUTO</b>

#### **Art. 4: Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi**

1. Ai sensi della normativa vigente<sup>2</sup>, l'Amministrazione è dotata del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, individuandolo nella Unità Organizzativa cui afferiscono le funzioni del Protocollo e dell'Archivio.
2. Al Servizio è preposto il Responsabile della predetta Unità Organizzativa.
3. Il Servizio svolge i seguenti compiti:

<sup>2</sup> Art. 61, cc. 1 e 2 del "TESTO UNICO"

- a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- c) garantisce la produzione e conservazione del registro giornaliero di protocollo;
- d) cura, di concerto con il Servizio Informatico, che le funzionalità del sistema, in caso di guasti o anomalie, vengano ripristinate entro 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- e) cura, di concerto con il Servizio Informatico, la conservazione delle copie di cui alla normativa vigente<sup>3</sup> in luoghi sicuri differenti;
- f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi;
- g) autorizza, con appositi provvedimenti, le operazioni di annullamento delle registrazioni di protocollo;
- h) vigila sull'osservanza delle disposizioni del presente Manuale di gestione da parte del personale autorizzato e degli incaricati;
- i) cura, ai sensi della normativa vigente<sup>4</sup>, il trasferimento dei documenti dagli uffici agli archivi e la conservazione degli archivi medesimi;
- j) cura il costante aggiornamento del presente Manuale di gestione e di tutti i suoi allegati.

## **Art. 5: Conservazione delle copie del registro informatico di protocollo**

1. Ai sensi della normativa vigente<sup>5</sup>, il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

## **Art. 6: Firma digitale qualificata. Abilitazione dei dipendenti**

1. Per l'espletamento delle attività istituzionali, qualora se ne abbia la necessità, l'Amministrazione fornisce la firma digitale o elettronica qualificata ai dipendenti da essa delegati a rappresentarla.

## **Art. 7: Caselle di Posta elettronica**

1. L'AOO è dotata della casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA); questa casella costituisce l'indirizzo virtuale dell'AOO e di tutti gli uffici che ad essa fanno riferimento.
2. Le caselle di Posta Elettronica Certificata sono accessibile, per l'invio e la ricezione di documenti, solo dall'Ufficio Protocollo, come specificato al successivo art. 16, mentre per la manutenzione e la gestione tecnica è accessibile al servizio Informatico.
3. Ogni Servizio è dotato di mail istituzionale certificata, le mail sono riportate nel sito istituzionale sezione "Trasparenza" secondo quanto stabilito dal D.L. 33/2013.

## **Art. 8: Sistema di classificazione dei documenti**

1. A seguito dell'introduzione del protocollo unico di cui al successivo art. 52 e per garantire la corretta classificazione e organizzazione dei documenti nell'archivio, a partire dalla fase corrente, viene adottato il "Titolario di classificazione" di cui al successivo art. 42.

<sup>3</sup> Artt. 62 e 63 del "TESTO UNICO"

<sup>4</sup> Artt. 67, 68 e 69 del "TESTO UNICO"

<sup>5</sup> Art. 7, comma 5, delle "REGOLE TECNICHE"

## II – PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

### Art. 9: Protocolli diversi dal protocollo informatico

1. Tutti i documenti inviati e ricevuti dall'Amministrazione sono registrati all'interno del registro di protocollo informatico.
2. Sono consentite, tuttavia, forme di registrazione particolari per alcune tipologie di documenti come specificato al successivo art. 39.

## III – PIANO PER LA SICUREZZA INFORMATICA

### Art. 10: Piano per la sicurezza informatica

1. Il Piano per la sicurezza informatica, redatto ai sensi della normativa vigente, è contenuto nel "Documento Programmatico sulla Sicurezza Informatica (DPS)", approvato dalla Giunta comunale con proprio atto, cui si fa rinvio.
2. E' messo in atto ai sensi della normativa vigente<sup>6</sup> il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi.

### Art. 11: Politiche di sicurezza

1. **Politiche accettabili di uso del sistema informativo.** Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, 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 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 dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.
2. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione. 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.
3. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati delle aziende outsourcer 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.

<sup>6</sup>Art. 4, lett. c, delle "REGOLE TECNICHE"

4. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito. Le singole aree o settori o Divisioni o Direzioni sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

5. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni. 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 dell'uso 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 sei mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.

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 l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia. Non permettere ai colleghi, né tanto meno ad esterni, di operare sulla propria postazione di lavoro con le proprie credenziali.

6. **Politiche – antivirus.** I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni. I danni causati dai virus all'Amministrazione, 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.

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

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

Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione. Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato. Non 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. Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati. Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura. Non scaricare mai messaggi da siti o sorgenti sospette. 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

dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus. Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiati dai CD/DVD in allegato a riviste. Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone. Evitare collegamenti diretti ad Internet via modem.

Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura. Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura. Non utilizzare i server di rete come stazioni di lavoro. Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali. Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione. 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 dell'Amministrazione ed, eventualmente, all'esterno. Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus. Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato. È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

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 dell'evoluzione delle tecnologie disponibili sul mercato.

**7. 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 l'evento 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 l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

**8. Politiche - uso non accettabile.** Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete). In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

- Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
- Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
- È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
- Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
- Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.

- Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedopornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
- Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
- Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
- Realizzare breccie nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per breccie della sicurezza si intendono, in modo riduttivo:
  - accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione, • attività di "sniffing";
  - disturbo della trasmissione;
  - spoofing dei pacchetti;
  - negazione del servizio;
  - le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
  - attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
- Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
- Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
- Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
- Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
- Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

**9. Attività di messaggistica e comunicazione.** Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).

- Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
- Uso non autorizzato delle informazioni della testata delle e-mail,
- Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare
- Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
- Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

## IV – MODALITA' DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DI DOCUMENTI

### Art. 12: Principi generali

1. Secondo quanto previsto dalla normativa vigente<sup>7</sup>, l'Amministrazione forma gli originali dei propri documenti con mezzi informatici.

<sup>7</sup>Artt 40 e 71 del C.A.D.

