*Ministero dell'Istruzione, dell'Università e della Ricerca*

# ISTITUTO COMPRENSIVO PERUGIA 14

# 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*

Sommario



**ALLEGATI:**

- NOMINA RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO
- SERVIZIO PER LA CONSERVAZIONE SOSTITUTIVA
- REGISTRO DI EMERGENZA
- REGISTRO DI ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

# AOO E MODELLO ORGANIZZATIVO

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO), composta dall'insieme di tutti gli UOP/UOR/UU articolati come di seguto riportato

## AREA OPERATIVA OMOGENEA (A.O.O.)

*Istituto comprensivo Perugia 14*

## UNITÀ ORGANIZZATIVE DI REGISTRAZIONE (U.O.P.)

**-PGIC85300B -**

*Ufficio di Protocollo (unico)*

## UNITÀ ORGANIZZATIVE DI RIFERIMENTO (U.O.R.)

*Articolazione degli uffici*

1) **Area Affari Generali**
2) **Area Didattica**
3) **Area Personale**
4) **Area Contabilità e Bilancio**
5) **Area Magazzino e Patrimonio**
6) **Dirigente**
7) **Direttore**

## UFFICIO UTENTE (U.U.)

*(soggetto destinatario del documento /flusso documentale)*

1) **Boriosi Marta (Dirigente)**
2) **Bussotti Elisabetta (Area Didattica)**
3) **Gaggi Clara (Area del Personale)**
4) **Morini Monia (Area del Personale)**
5) **Orselli Sabrina (Area del Personale)**
6) **Tardocchi Giuseppe (Area Contabilità e Bilancio / Magazzino e Patrimonio)**
7) **Tosti Cinzia (Affari generali)**
8) **Truffelli Romano (Area Didattica)**

**Considerazioni:**

• All'interno della AOO il sistema di protocollazione è **unico**.

• Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Nel medesimo allegato sono riportati la denominazione, il codice identificativo della AOO e l'insieme degli UOR che la compongono con la loro articolazione in UU.

All'interno della AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in entrata e in uscita; pertanto ogni UOR svolge anche i compiti di UOP.

# ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Sono escluse dalla protocollazione, ai sensi dell'art. 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 d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a reg. particolare
- convocazioni ad incontri o riunioni e corsi di formazione interni
- delibere, disposizioni interne, documenti interni informali
- ricevute di ritorno delle raccomandate A.R

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

1. La corrispondenza viene quotidianamente raccolta dal servizio postale pubblico dal personale dell'Ufficio Posta della UOP dell'Amministrazione/AOO entro le ore 11:30 di ogni giorno;
2. La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, viene consegnata in busta chiusa al servizio postale pubblico alle ore 12:30. (o in alternativa, in occasione della raccolta della corrispondenza) di ogni giorno;
3. Gli Uffici Utente devono far pervenire la posta in partenza all'Ufficio Posta della UOP generale che esegue la spedizione, entro e non oltre le ore 11:00 di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal RSP che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

# 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 all'interno dell'Amministrazione/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 l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto

ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE :

- 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 dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 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 dall'art. 24 della legge 7 agosto 1990 n. 241, dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

# PIANO DI CONSERVAZIONE E MASSIMARIO DI SCARTO

| TIPOLOGIA | CONSERVAZIONE |
|---|---|
| ACCERTAMENTO CERTIFICAZIONE DI QUALITA' | ∞ |
| ACCERTAMENTO SANITARIO | ∞ |
| ACCERTAMENTO TECNICO PER MALATTIE PROF.LI | ∞ |
| ACCORDO DI RETE CON SCUOLE O ENTI | ∞ |
| ACQUISTO IMMOBILE | ∞ |
| ALBO DEL PERSONALE | ∞ |
| ALLEGATO DOCUMENTO VALUTAZIONE RISCHI | ∞ |
| ANNUARIO SCOLASTICO | ∞ |
| ASSEGNAZIONE SEDE | ∞ |
| ATTESTATO PARTECIPAZIONE CORSO FORMAZIONE E AGGIORNAMENTO | ∞ |
| ATTO ACCORPAMENTO SCUOLE | ∞ |
| ATTO COSTITUTIVO COOP. ALUNNI | ∞ |
| ATTO DI SCARTO DOCUMENTI | ∞ |
| ATTO ELEZIONE OO.CC. | ∞ |
| AUTORIZZAZIONE COLLABORAZIONE PLURIMA | ∞ |
| AUTORIZZAZIONE DI SICUREZZA LOCALI | ∞ |
| AUTORIZZAZIONE ESERCIZIO LIBERA PROFESSIONE | ∞ |
| AUTORIZZAZIONE LEZIONI PRIVATE | ∞ |
| BANDO BORSA DI STUDIO | ∞ |
| BANDO PER STAGE | ∞ |
| BILANCIO ANNUALE | ∞ |
| BORSA DI STUDIO | ∞ |
| CARTA DEI SERVIZI | ∞ |
| CATOLOGO BIBLIOTECA | ∞ |
| CERTIFICATO DI RESIDENZA | ∞ |
| CERTIFICATO DI SANA E ROBUSTA COSTITUZIONE | ∞ |
| CERTIFICATO DI SERVIZIO DEL PERSONALE | ∞ |
| CERTIFICATO DI STUDIO | ∞ |
| CERTIFICATO NASCITA | ∞ |
| CERTIFICAZIONE DI QUALITA' | ∞ |
| CERTIFICAZIONE DI SICUREZZA IMPIANTI | ∞ |
| CIRCOLARE INTERNA | ∞ |
| CONTO CONSUNTIVO | ∞ |
| CONTRATTO ASSUNZIONE PERSONALE | ∞ |
| CONTRATTO COSTRUZIONE | ∞ |
| CONTRATTO DI COSTRUZIONE | ∞ |
| CONTRATTO ESPLETAMENTO DI SERVIZI | ∞ |
| CONTRATTO FORNITURA MATERIALE | ∞ |
| CONTRATTO INDIVIDUALE | ∞ |
| CONTRATTO PER FORNITURA DI MATERIALE | ∞ |
| CONTRATTO PRESTAZIONE DI VARIA NATURA | ∞ |
| CONTRATTO RISTRUTT. MANUTENZIONE | ∞ |
| CONVENZIONE DI CASSA CASSIERE ISTITUTO | ∞ |
| CORRISPONDENZA ARRIVO | ∞ |
| CORRISPONDENZA RELATIVA A COOP. ALUNNI | ∞ |
| CORRISPONDENZA USCITA | ∞ |
| DECRETO ASPETTATIVA | ∞ |
| DECRETO DELEGATO | ∞ |
| DECRETO DI ASSENZA | ∞ |
| DECRETO DI NOMINA | ∞ |

| | |
|---|---|
| DECRETO DI TRASFERIMENTO | ∞ |
| DECRETO PER CONGEDO MATERNITA' ANTICIPATA | ∞ |
| DECRETO PER CONGEDO PARENTALE | ∞ |
| DECRETO PER CONGEDO STRAORDINARIO | ∞ |
| DELIBERA COMITATO SCOLASTICO | ∞ |
| DETERMINA DEL DIRIGENTE | ∞ |
| DIPLOMA | ∞ |
| DISEGNO IMMOBILE DI PROPRIETA' | ∞ |
| DISEGNO TECNICO IMPIANTI O ATTREZZATURE | ∞ |
| DISOGNO IMMOBILE IN USO | ∞ |
| DISPENSA AGGIORNAMENTO PERSONALE | ∞ |
| DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA INVALSI | ∞ |
| DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA OCSE | ∞ |
| DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA RAV | ∞ |
| DOC RELATIVO A ATTIVITA' DI VALUTAZIONE SCOLASTICA SIDI | ∞ |
| DOC RELATIVO A PROGETTO OCSEA | ∞ |
| DOC. ACQUISITA PER CONCILIAZIONE | ∞ |
| DOC. AGGIORNAMENTO PERSONALE | ∞ |
| DOC. AMBITI DISCLIPINARI OO.CC | ∞ |
| DOC. ASSISTENZA SCOLASTICA | ∞ |
| DOC. AZIONE LEGALE DIPENDENTE | ∞ |
| DOC. COMODATO IMMOBILE | ∞ |
| DOC. CONGEDO PARENTALE | ∞ |
| DOC. CONGEDO PER ASPETTATIVA | ∞ |
| DOC. CONGEDO PER MATERNITA' | ∞ |
| DOC. CONGEDO PER MATERNITA' ANTICIPATA | ∞ |
| DOC. CONGEDO STRAORDINARIO | ∞ |
| DOC. CONSULENZA COLLABORAZIONE ENTE LOCALE | ∞ |
| DOC. CONSULENZA ESPERTO ESTERNO | ∞ |
| DOC. CONSULENZA ISTITUZIONI ENTI VARI | ∞ |
| DOC. DELIBERATIVO A COOP. ALUNNI | ∞ |
| DOC. DIRITTO ALLO STUDIO | ∞ |
| DOC. GRUPPO DI LAVORO OO.CC | ∞ |
| DOC. INSERIMENTO ALUNNI STRANIERI | ∞ |
| DOC. INTITOLAZIONE SCUOLA | ∞ |
| DOC. ISTRUTTORIO COMITATO SCOLASTICO | ∞ |
| DOC. ISTRUTTORIO COMMISSIONE OO.CC | ∞ |
| DOC. ISTRUTTORIO PER COOP. ALUNNI | ∞ |
| DOC. POSIZIONE PREVIDENZIALE | ∞ |
| DOC. POSIZIONE STIPENDIALE | ∞ |
| DOC. POSIZIONE TRIBUTARIA | ∞ |
| DOC. PRESA DI SERVIZIO | ∞ |
| DOC. PRODOTTA PER CONCILIAZIONE | ∞ |
| DOC. PRODOTTO DA ALUNNI PER ATT. DIDATTICHE | ∞ |
| DOC. PRODOTTO DA DOCENTI PER ATT. DIDATTICHE | ∞ |
| DOC. PRODOTTO DA DOCENTI PER PROGETTO FORMATIVO | ∞ |
| DOC. PRODOTTO DA DOCENTI PER SPERIMENTAZIONE MULTISCIPLINARE | ∞ |
| DOC. PRODOTTO DA STUDENTI PER PROGETTO FORMATIVO | ∞ |
| DOC. PRODOTTO DA STUDENTI PER SPERIMENTAZIONE MULTISCIPLINARE | ∞ |
| DOC. PROGETTI FORMATIVI | ∞ |
| DOC. PROGETTI FORMATIVI DI RECUPERO | ∞ |
| DOC. PROGETTO INVALSI | ∞ |
| DOC. RELATIVA A IMMOBILI DI PROPRIETA' | ∞ |
| DOC. RELATIVA A SCIOPERI | ∞ |

| | |
|---|---|
| DOC. RELATIVO A ATT. FORMATIVA O PARASCOLASTICA | ∞ |
| DOC. RELATIVO A ATTREZZAURE PER IMMOBILI DI PROPRIETA' | ∞ |
| DOC. RELATIVO A BORSA DI STUDIO | ∞ |
| DOC. RELATIVO A CESSIONE DEL QUINTO | ∞ |
| DOC. RELATIVO A CONTRATTAZIONE D'ISTITUTO | ∞ |
| DOC. RELATIVO A CONVENZIONI PER ATTIVITA' FORMATIVE E/O PARASCOLASTICHE | ∞ |
| DOC. RELATIVO A CONVENZIONI PER EDUCAZIONE ALLA SALUTE | ∞ |
| DOC. RELATIVO A EDUCAZIONE ALLA SALUTE | ∞ |
| DOC. RELATIVO A GRUPPI DI LAVORO OO.CC. | ∞ |
| DOC. RELATIVO A IMMOBILI DI PROPRIETA' | ∞ |
| DOC. RELATIVO A IMMOBILI IN USO | ∞ |
| DOC. RELATIVO A INAUGURAZIONI | ∞ |
| DOC. RELATIVO A INCHIESTA AMBIENTALI SOCIO/ECONOMICHE | ∞ |
| DOC. RELATIVO A MALATTIA PROFESSIONALE | ∞ |
| DOC. RELATIVO A MONITORAGGIO | ∞ |
| DOC. RELATIVO A PATRONATO SCOLASTICO | ∞ |
| DOC. RELATIVO A PENSIONE | ∞ |
| DOC. RELATIVO A PERCORSO DIDATTICO PRODOTTO DA DOCENTI | ∞ |
| DOC. RELATIVO A PERCORSO DIDATTICO PRODOTTO DA STUDENTI | ∞ |
| DOC. RELATIVO A PROGETTI DI EDUCAZIONE ALLA SALUTE | ∞ |
| DOC. RELATIVO A PROGETTI FORMATIVI | ∞ |
| DOC. RELATIVO A PROGETTI FORMATIVI TEATRALI | ∞ |
| DOC. RELATIVO A PROGETTI TRIMESTRALI O QUADRIMESTRALI | ∞ |
| DOC. RELATIVO A PROGETTO FORMATIVO MUSICALE | ∞ |
| DOC. RELATIVO A PROGETTO FORMATIVO ORIENTAMENTO | ∞ |
| DOC. RELATIVO A RAPPORTI CON ORGANIZZAZIONE SINDACALE | ∞ |
| DOC. RELATIVO A RAPPRESENTANZE SINDACALI INTERNE | ∞ |
| DOC. RELATIVO A RISTRUTTURAZIONE IMMOBILE | ∞ |
| DOC. RELATIVO A STAGE | ∞ |
| DOC. RELATIVO A STAGE | ∞ |
| DOC. RELATIVO A STATO DI FAMIGLIA | ∞ |
| DOC. RELATIVO A TRASFORMAZIONE SCUOLA | ∞ |
| DOC. RELATIVO A TRATTATO DI QUIESCENZA | ∞ |
| DOC. RISCATTO PERIODO ASSICURATIVO | ∞ |
| DOC. VALUTAZIONE RISCHI | ∞ |
| DOC. VISITA COLLEGIALE | ∞ |
| DOC. VISITA FISCALE | ∞ |
| DOCUMENTAZIONE INFORTUNIO | ∞ |
| DOCUMENTO PRODOTTO DA DOCENTI PER SUSSIDI | ∞ |
| DOCUMENTO PRODOTTO DA STUDENTI PER SUSSIDI | ∞ |
| DOCUMENTO PROGRAMMATICO SICUREZZA | ∞ |
| DOMANDA DI SCATTO ANTICIPATO | ∞ |
| DOMANDA DI TRASFERIEMENTO | ∞ |
| DONAZIONE IMMOBILE | ∞ |
| ELABORATI DEGLI ALUNNI | ∞ |
| ELABORATO PROVA SCRITTA O GRAFICA DI ESAME | ∞ |
| ELENCO DI CONSISTENZA BENE INVENTARIATO | ∞ |
| ELENCO PERSONALE | ∞ |
| FASCICOLO ATA | ∞ |
| FASCICOLO PERSONALE ALUNNO | ∞ |
| FASCICOLO PERSONALE DOCENTE | ∞ |
| GARANZIA APPARECCHIATURE | ∞ |
| GIORNALE DI CASSA | ∞ |
| GIORNALINO DI CLASSE | ∞ |
| INVENTARIO PATRIMONIALE BENI | ∞ |

| | |
|---|---|
| LETTERA DI INVITO AL DIPENDENTE | ∞ |
| LIBRETTO SCOLASTICO | ∞ |
| LIBRO GIORNALE CASSA SCOLASTICA | ∞ |
| LOCANDINA STAMPATA O PUBBLICATA DA O PER CONTO DELLA SCUOLA | ∞ |
| MODELLO 01/M | ∞ |
| MODELLO 101 | ∞ |
| MODELLO CUD | ∞ |
| MODLELLO 26 CG | ∞ |
| NOMINA A COMMISSIONE OO.CC. | ∞ |
| NOMINA A GRUPPO DI LAVORO | ∞ |
| NOMINA COMITATO SCOLASTICO | ∞ |
| NORME ARCHIVIO SCOLASTICO | ∞ |
| NORME BIBLIOTECA | ∞ |
| ORARIO DELLE LEZIONI | ∞ |
| ORDINANZA INTERNA | ∞ |
| ORDINE DI SERVIZIO GENERALE | ∞ |
| PAGELLA SCOLASTICA | ∞ |
| PARTITARIO ENTRATE | ∞ |
| PEI | ∞ |
| PERMESSO BREVE DEL PERSONALE | ∞ |
| PERMESSO DI STUDIO DEL PERSONALE | ∞ |
| PIANO DI LAVORO | ∞ |
| PIANTA ORGANICA | ∞ |
| PLANIMETRIA IMMOBILE DI PROPRIETA' | ∞ |
| PLANIMETRIA IMMOBILE IN USO | ∞ |
| POF | ∞ |
| PON | ∞ |
| POR | ∞ |
| PORTFOLIO | ∞ |
| PRATICA PER ASSISTENZA COLONIA | ∞ |
| PROGETTO TECNICO | ∞ |
| PROGETTO TECNICO IMPIANTI O ATTREZZATURE | ∞ |
| PROGRAMMA CONTABILE ANNUALE | ∞ |
| PROGRAMMA D'ESAME | ∞ |
| PROGRAMMA DOCENTE | ∞ |
| PUBBLICAZIONE VARIA DELLA SCUOLA | ∞ |
| QUESTIONARIO | ∞ |
| RASSEGNA STAMPA SCUOLA | ∞ |
| RAV | ∞ |
| REFERTO VISITA COLLEGIALE | ∞ |
| REFERTO VISITA FISCALE | ∞ |
| REGISTRIO CRONOLOGICO DEI CONTRATTI | ∞ |
| REGISTRO CARICO E SCARICO DEI DIPLOMI | ∞ |
| REGISTRO CONSEGNA DIPLOMI | ∞ |
| REGISTRO CONTRATTI FORNITURA MATERIALE | ∞ |
| REGISTRO DEI CERTIFICATI | ∞ |
| REGISTRO DEI CONTRATTI | ∞ |
| REGISTRO DEI VERBALI OO.CC. | ∞ |
| REGISTRO DELIBERAZIONI | ∞ |
| REGISTRO DI CLASSE | ∞ |
| REGISTRO DI ENTRATA BIBLIOTECA | ∞ |
| REGISTRO DI ENTRATA SUSSIDI MULTIMEDIALI | ∞ |
| REGISTRO DI STATO DEL PERSONALE | ∞ |
| REGISTRO GENERALE DEI VOTI | ∞ |
| REGISTRO INFORTUNI | ∞ |
| REGISTRO ISCRIZIONE ALUNNI | ∞ |

| | |
|---|---|
| REGISTRO LICENZE SOFTWARE | ∞ |
| REGISTRO MODELLI AT | ∞ |
| REGISTRO OPERAZIONI CONTO CORRENTE BANCARIO | ∞ |
| REGISTRO OPERAZIONI CONTO CORRENTE POSTALE | ∞ |
| REGISTRO PROFILO ALUNNO | ∞ |
| REGISTRO PROTOCOLLO | ∞ |
| REGISTRO RIUNIONI PER DIPARTIMENTO | ∞ |
| REGISTRO RIUNIONI PER MATERIA | ∞ |
| REGISTRO SPESE PER APERTURA CREDITO | ∞ |
| REGISTRO STIPENDI | ∞ |
| REGISTRO STIPENDI | ∞ |
| REGISTRO VERBALI CASSA SCOLASTICA | ∞ |
| REGISTRO VERBALI CONSIGLIO DI AMMINISTRAZIONE | ∞ |
| REGISTRO VERBALI CONTRATTAZIONE D'ISTITUTO | ∞ |
| REGISTRO VERBALI DEL COLLEGIO DEI REVISORI | ∞ |
| REGISTRO VERBALI ESAME DI STATO | ∞ |
| REGISTRO VERBALI PROVE D'ESAME | ∞ |
| REGOLAMENTO BIBLIOTECA | ∞ |
| REGOLAMENTO INTERNO LABORATORIO | ∞ |
| REL. COLL.NE ASSOCIAZIONI E COOPERATIVE | ∞ |
| RELAZIONE ADOZIONE LIBRO DI TESTO | ∞ |
| RELAZIONE COLLABORAZIONE ENTE LOCALE | ∞ |
| RELAZIONE COLLABORAZIONE ESPERTO ESTERNO | ∞ |
| RELAZIONE COLLABORAZIONE ISTITUZIONI SOCIO ASSISTENZIALI | ∞ |
| RELAZIONE CONSULENZA SSN | ∞ |
| RELAZIONE CONSULENZA TRIBUNALE DEI MINORI | ∞ |
| RELAZIONE ESTERNA | ∞ |
| RELAZIONE FINALE DI CLASSE | ∞ |
| RELAZIONE FINALE D'ISTITUTO | ∞ |
| RELAZIONE RIPETENZA ALUNNI | ∞ |
| RELAZIONE SU COLLABORAZIONE COOP. E ASSOCIAZIONI | ∞ |
| RELAZIONE SU COLLABORAZIONE SSN | ∞ |
| RELAZIONE SU CONSULENZE COOP. E ASSOCIAZIONI | ∞ |
| RELAZIONECOLLABORAZIONE TRIBUNALE DEI MINORI | ∞ |
| RENDICONTO TRIMESTRALE | ∞ |
| REPERTORIO D'ARCHIVIO | ∞ |
| REPERTORIO FASCICOLI D'ARCHIVIO | ∞ |
| RICOGNIZIONE PATRIMONIALE DECENNALE | ∞ |
| RICOGNIZIONE PATRIMONIALE DI SCUOLA CONFLUITA | ∞ |
| RICORSO AMMINISTRATIVO | ∞ |
| RIVALUTAZIONE PATRIMONIALE QUINQUENNALE | ∞ |
| RSU | ∞ |
| RUBRICA ALFABETICA DEL PROTOCOLLO | ∞ |
| RUOLO DEL PERSONALE | ∞ |
| SCHEDA ALUNNO | ∞ |
| SCHEDARIO ALUNNI | ∞ |
| STATISTICA | ∞ |
| STATO DI FAMIGLIA | ∞ |
| STATUTO E REGOLAMENTO | ∞ |
| TESSERA MINISTERIALE | ∞ |
| TITOLO DI STUDIO | ∞ |
| TRATTAMENTO QUIESCENZA | ∞ |
| VERBALE ADOZIONE LIBRI DI TESTO | ∞ |
| VERBALE CASSA SCOLASTICA | ∞ |
| VERBALE COMITATO SCOLASTICO | ∞ |
| VERBALE COMMISSIONE ELETTORALE OO.CC. | ∞ |

| | |
|---|---|
| VERBALE COMMISSIONE OO.CC. | ∞ |
| VERBALE CONSIGLIO DI AMMINISTRAZIONE E DI PRESIDENZA | ∞ |
| VERBALE CONTRATTAZIONE D'ISTITUTO | ∞ |
| VERBALE DEL COLLEGIO DEI REVISORI | ∞ |
| VERBALE DI COLLAUDO | ∞ |
| VERBALE DI COLLAUDO ATTREZZATURA | ∞ |
| VERBALE DI CONSEGNA BENE INVENTARIATO | ∞ |
| VERBALE GRUPPO DI LAVORO OO.CC. | ∞ |
| VERBALE ISPETTORI SCOLASTICI | ∞ |
| VERBALE ORGANO COLLEGIALE | ∞ |
| VERBALE PASSAGGIO DI CONSEGNA | ∞ |
| VERBALE PROVA D'ESAME | ∞ |
| ACCONTO AL PERSONALE | 50 |
| ATTO COSTITUTIVO COLLEGIO REVISORI | 50 |
| ATTO RELATIVO A LOCAZIONE IMMOBILI | 50 |
| CONTRATTO DI PRESTAZIONE D'OPERA | 50 |
| DENUNCIA ANNUALE IRAP | 50 |
| DENUNCIA MENSILE ANALITICA | 50 |
| DENUNCIA RETRIBUTIVA MENSILE | 50 |
| DISPOSIZIONE CCNL | 50 |
| DISPOSIZIONE PERSONALE | 50 |
| DOC. COMPENSO A VARIO TITOLO | 50 |
| DOC. CONGUAGLIO PER IL PERSONALE | 50 |
| DOC. FONDO ESPERO | 50 |
| DOC. PER CONSULENZA LIQUIDAZIONE | 50 |
| DOC. REGOLARIZZANTE CONTRIBUTIVA PERSONALI | 50 |
| DOC. RELATIVO A CONTRIBUTI INPS | 50 |
| DOC. RELATIVO A RECUPERO RETRIBUZIONE | 50 |
| EMENS | 50 |
| MODELLO 770 | 50 |
| NORMA CCNL | 50 |
| REGISTRO ASSENZE PERSONALE | 50 |
| TABELLA STIPENDIO | 50 |
| TABULATO MENSILE RIEPILOGATIVO RETRIBUZIONE | 50 |
| TABULATO RIEPILOGATO IMPONIBILE | 50 |
| ACQUISTO ATTREZZATURA | 10 |
| BOLLETTARIO CARICO SCARICO | 10 |
| BOLLETTINO CC/POSTALE | 10 |
| BUONO D'ORDINE | 10 |
| COPIA DELIBERA LIQUIDAZIONE | 10 |
| COPIA DETERMINA DI LIQUIDAZIONE | 10 |
| COPIA DI DELIBERE DI LIQUIDAZIONE | 10 |
| CORRISPONDENZA RELATIVA A ACQUISTI | 10 |
| CORRISPONDENZA RELATIVA A INTERVENTI DI MANUTENZIONE | 10 |
| DISTINTA TRASMISSIONE AL TESORIERE MANDATI | 10 |
| DISTINTA TRASMISSIONE AL TESORIERE REVERALI | 10 |
| DISTINTA TRASMISSIONE TESORERIA | 10 |
| DO. RELATIVA A REVERSALE DI PAGAMENTO | 10 |
| DOC. GIUSTIFICATIVO A MANDATO DI PAGAMENTO | 10 |
| DOC. RELATIVA A CERIMONIA | 10 |
| DOC. RELATIVA A INTERVENTI DI MANUTENZIONE | 10 |
| DOC. RELATIVA A NOMINA CASSIERE ISTITUTO | 10 |
| DOC. RELATIVA A RECUPERO ORARIO | 10 |
| ELENCO ALUNNI | 10 |
| ESTRATTO CONTO BANCARIO | 10 |
| ESTRATTO CONTO POSTALE | 10 |
| FATTURA | 10 |

| | |
|---|---|
| FOGLIO DI PRESENZA | 10 |
| GRADUATORIA D'ISTITUTO | 10 |
| GRADUATORIA NON IN VIGORE | 10 |
| LICENZA SOFTWARE | 10 |
| MANDATO DI PAGAMENTO | 10 |
| ORDINATIVO ACQUISTO | 10 |
| REGISTRO ATTIVITA' GRUPPO SPORTIVO | 10 |
| REGISTRO DEBITI FORMATIVI | 10 |
| REGISTRO POSTA IN PARTENZA E IN ARRIVO | 10 |
| REGISTRO TASSE SCOLASTICHE PER ISCRIZIONE E DIPLOMA | 10 |
| REVERSALE DI PAGAMENTO | 10 |
| UTENZA ELETTRICA | 10 |
| UTENZA TASSA RIFIUTI | 10 |
| UTENZA TELEFONO | 10 |
| VERBALI DEBITO FORMATIVO | 10 |
| ABB. A GIORNALE | 6 |
| ABB. A PUBBLICAZIONE | 6 |
| ABB. A RIVISTA | 6 |
| ACQUISTO GIORNALE | 6 |
| ACQUISTO LIBRI | 6 |
| ACQUISTO MATERIALE DI CONSUMO | 6 |
| ACQUISTO PUBBLICAZIONE | 6 |
| ACQUISTO RIVISTA | 6 |
| ATTESTAZIONE PAGAMENTO SERVIZIO DI TRASPORTO | 6 |
| AUTORIZZAZIONE ALL'USO DI IMPIANTI SPORTIVI | 6 |
| AUTORIZZAZIONE USO LOCALI SCOLASTICI | 6 |
| BOLLETTARIO RICHIESTA STAMPATI | 6 |
| BUONI LIBRI, DOC. DI SUPPORTO | 6 |
| BUONO LIBRO | 6 |
| CEDOLA LIBRARIA | 6 |
| CERTIFICATO NASCITA | 6 |
| CERTIFICATO NASCITA E VACCINAZIONE ALUNNO | 6 |
| CERTIFICATO VACCINAZIONE | 6 |
| CONVOCAZIONE RIUNIONE OO.CC. | 6 |
| COPIA DI CERTIFICATO | 6 |
| DOC. PRODOTTA DA CANDITATO A ESAME | 6 |
| DOC. RELATIVA A GITE SCOLASTICHE | 6 |
| DOC. RELATIVI A CAMPAGNE DI DISINFESTAZIONE/VACCINAZIONE | 6 |
| DOC. RELATIVO A MANFESTAZIONE TEATRALE | 6 |
| DOC. RELATIVO A ATTIVITA' SCOLASTICA ESTERNA | 6 |
| DOC. RELATIVO A ATTIVITA' SCOLASTICA INTERNA | 6 |
| DOC. RELATIVO A BUONI ACQUISTI GENERE DI REFEZIONE E CONSUMO | 6 |
| DOC. RELATIVO A CAMPAGNE DISINFESTAZIONE | 6 |
| DOC. RELATIVO A CAMPAGNE VACCINAZIONE | 6 |
| DOC. RELATIVO A CONTRIBUTI ALLA BIBLIOTECA SCOLASTICA | 6 |
| DOC. RELATIVO A CONTRIBUTI BIBLIOTECA | 6 |
| DOCUMENTI PER ISCRIZIONI | 6 |
| DOMANDA AMMISSIONE A ESAME | 6 |
| DOMANDA ISCRIZIONE | 6 |
| ELENCO BUONI LIBRI CONCESSI | 6 |
| ELENCO PRESENZE MENSA | 6 |
| LIBRETTO AUTOMOBILE | 6 |
| MATRICE DI BUONI ACQUISTO PER GENERI DI REFEZIONE E CONSUMO | 6 |
| NOMINA OO.CC | 6 |

| | |
|---|---|
| REGISTRO ASSENZE ALUNNI | 6 |
| REGISTRO ELZIONE PRIVATE | 6 |
| RICHIESTA CONSULTAZIONE ARCHIVIO | 6 |
| RICHIESTA DI CERTIFICATO | 6 |
| RICHIESTA DI FERE | 6 |
| RICHIESTA DI INTERVENTO | 6 |
| RICHIESTA DI RISORSE STRUMENTALI | 6 |
| RICHIESTA DI TRASPORTO GRATUITO | 6 |
| RICHIESTA INTERVENTO DOTAZIONE STRUMENTALE | 6 |
| RICHIESTA ISCRIZIONE MENSA | 6 |
| RICHIESTA ISCRIZIONE SERVIZIO DI TRASPORTO ALUNNI | 6 |
| RICHIESTA STAMPATI | 6 |
| VISITA DI STUDIO | 6 |
| ABB. FERROVIARIO O DIVERSO | 1 |
| COMPITO IN CLASSE | 1 |
| ELABORATO PROVE PRATICA ESAME | 1 |
| GRADUATORIA IN CALCE | 1 |
| REGISTRO IMMATRICOLAZIONE ALUNNI | 1 |
| RICHIESTA ACCESSO A DOCUMENTI | 1 |
| RICHIESTA COPIA DI ATTI | 1 |
| RISCHIESTA SUPPLENZA | 1 |

# MODULO DI CONSULTAZIONE DELLA SEZIONE DI DEPOSITO E STORICA DELL'ARCHIVIO

**Spett.le Dirigente Scolastico**
**ISTITUTO COMPRENSIVO PERUGIA 14**

**Oggetto:** Richiesta di consultazione del materiale documentario conservato nella sezione di deposito/storica dell'Archivio generale dell'Amministrazione.

**Scopo della consultazione**:
.....
.....

**Durata indicativa della consultazione:** ..... mesi

**Materiale da consultare**:
o **Titolo** .....
o **Classe** .....
o **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 .....

o **Descrizione degli inserti:**
- Oggetto del fascicolo:.....
- Anno di repertoriazione.....
- Dal numero ..... al numero.....

NOTE:
.....
.....

Perugia,

**L'OPERATORE RICEVENTE:**

.....

**IL RESPONSABILE DELL'ARCHIVIO**

.....

# POLITICHE DI SICUREZZA

POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATICO

## 1.1 Premessa

1. L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è 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.

2. 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.

3. 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.

## 1.2 Scopo

1. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.

2. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.

3. 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.

## 1.3 Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...), includendo tutto il personale affiliato con terze parti.

2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

## 1.4 Politiche – Uso generale e proprietà

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

### 1.5 Politiche Sicurezza e proprietà dell'informazione

1. 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.

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 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 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 l'attivazione 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 dall'Amministrazione.

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 dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.

7. 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.

8. 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.

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 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.

## 2.2 Scopo

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.

## 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 dell'Amministrazione 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 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 copiato 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.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico… [omissis]…che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- 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.

### 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 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.

## 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 all'interno dell'Amministrazione (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 dell'Amministrazione.
3. 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.

### 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, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
2. 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.
3. È rigorosamente proibita l'esportazione 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 dell'Amministrazione.
5. 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.
6. Usare un sistema dell'Amministrazione (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 dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione 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 "sniffing";
   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 l'accesso ai servizi di ogni altro utente abilitato.

13. 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.

14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

### 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 "messaggi spazzatura", 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 l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione 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 dell'Amministrazione.

### 4.2 Ambito di applicazione

1. Queste politiche sono relative solo a quelle linee che sono terminate all'interno della/e sede/i dell'Amministrazione. 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 – Scenari di impatto sull'Amministrazione

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 dell'Amministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

### 4.4 Politiche – Telefax

1. Dovrebbero essere adottate le seguenti regole:

- le linee fax dovrebbero essere approvate solo per uso istituzionale;
- nessuna linea dei telefax dovrebbe essere usata per uso personale;

2. Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.

3. Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensitività dei dati.

### 4.5 Politiche – 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 l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

### 4.6 Politiche – Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

- una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;
- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato;
- che cosa la connessione esterna richiede per essere acceduta.

## 5 POLITICHE PER L'INOLTRO 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 dell'Amministrazione

### 5.2 Ambito di applicazione

1. Queste politiche riguardano l'inoltro 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 all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.
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 dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno 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 dell'Amministrazione e le persone terze autorizzate (clienti, venditori, altre amministrazioni, cittadini, etc.) possono utilizzare la linea commutata per guadagnare l'ingresso alla Intranet dell'Amministrazione. 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 dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" 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 dell'Amministrazione.
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 L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

### 7.1 Scopo

1. Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

### 7.2 Ambito di applicazione

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

### 7.3 Politiche – Usi proibiti

1. Il sistema di posta dell'Amministrazione 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 – Uso personale

1. È considerato accettabile l'uso personale della posta istituzionale dell'Amministrazione a condizione che:
   - i messaggi personali siano archiviati in cartelle separate da quelle di lavoro;
   - venga utilizzata una ragionevole quantità di risorse pubbliche;
   - non si avviino catene di lettere o messaggi scherzosi, di disturbo o di altro genere.
2. Il personale dell'Amministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.
3. L'Amministrazione può però controllare senza preavviso i messaggi che transitano in rete per verificare il rispetto delle politiche concernenti gli "usi proibiti" di cui sopra.
4. Non è ammesso l'uso 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 l'accesso alla rete dell'Amministrazione 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 all'Amministrazione.

### 8.2 Ambito di applicazione

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

### 8.3 Politiche – Registrazione delle schede di accesso

1. Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing). Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

### 8.4 Politiche – Approvazione delle tecnologie

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

# PIANO FORMATIVO PER IL PERSONALE

- **Amministrazione:** ISTITUTO COMPRENSIVO PERUGIA 14

Tenute presenti le disponibilità di bilancio, in relazione anche al combinato disposto dell'art. 2 del CCNL 31 marzo 1999 e dell'art. 4 del CCNL 1 aprile 1999, nella impossibilità di organizzare autonomi corsi, è favorita l'adesione a corsi di formazione organizzati, per il personale dei servizi informatici e per quello impegnato nelle attività di registrazione del protocollo, dalle amministrazioni centrali o territoriali, nonché da aziende di sviluppo software

# 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 dell'art. 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 dell'art. 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 dell'articolo 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 dell'art. 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 dell'art. 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 – "Art. 17 del DPR 10 novembre 1997, n. 513 Utilizzo della firma digitale nelle pubbliche amministrazioni".
11. *Decreto legislativo 30 marzo 2001*, n. 165 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche".
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 "Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428" 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 l'innovazione 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 l'innovazione e le tecnologie, 9 dicembre 2002* -Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.
18. *Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre* 2002 Linee guida in

materia di digitalizzazione dell'amministrazione.

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 dell'articolo 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 l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249)
23. *Direttiva del Ministro per l'innovazione 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 dell'amministrazione per l'anno 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 dell'art. 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 all'Amministrazione 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 NELL'AOO | ESTREMI E DESCRIZIONE DELLA DELEGA RICEVUTA |
|---|---|---|
| **Prof.ssa Marta Boriosi** | Dirigente | |
| **Rag. Giuseppe Tardocchi** | D. S. G. A. | |
| | | |
| | | |
| | | |
| | | |

# ISTITUTO COMPRENSIVO "PERUGIA 14"

**Codice Meccanografico: PGIC85300B | Codice Fiscale: 94152410547**

Scuola dell'infanzia di Bosco, Montelaguardia, Ponte Felcino e Villa Pitignano
Scuola Primaria di Colombella, Montelaguardia, Ponte Felcino e Villa Pitignano
Scuola Secondaria di I° grado "Bonazzi - Lilli"


A Direttore S.G.A.
Giuseppe Tardocchi
Agli Atti

**OGGETTO:** **Oggetto: Nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi e del suo Vicario.**

## IL DIRIGENTE SCOLASTICO

**PREMESSO** che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi e delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

**VISTO** in particolare l'articolo 61, comma 2, il quale tra l'altro, stabilisce che presso il servizio gratuito del protocollo informatico, è preposto un dirigente, ovvero un funzionario, comunque in possesso di idonei requisiti professionali e di professionalità tecnico archivistica;

**VISTO** il Decreto ministeriale 14 ottobre 2003 "Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi", nel quale sono indicati gli adempimenti delle amministrazioni relativamente al protocollo informatico ed alla gestione dei procedimenti amministrativi con tecnologie informatiche;

**VISTI** i consequenziali adempimenti derivanti da quanto fin qui riportato;

**Ritenuto** che la S.V. possiede i requisiti necessari per procedere all'affidamento dell'incarico di cui alla presente;

**INCARICA LA S.V.**

1. in qualità di Direttore dei Servizi Generali e Amministrativi, quale Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi ai sensi dell'articolo 61 comma 2 del DPR n. 445/2000 con i compiti di seguito specificati:

• predisporre lo schema del Manuale di gestione del protocollo informatico;

• provvedere alla pubblicazione del Manuale anche su Internet;

• predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il Dirigente Scolastico;

• attribuire il livello di autorizzazione di ciascun addetto all'accesso alle funzioni delle procedure applicative di gestione del protocollo informatico e gestione documentale distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento, alla modifica e alla cancellazione delle informazioni;

• garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;

• garantire la corretta produzione e conservazione del registro giornaliero di protocollo;

• garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;

• curare, anche attraverso il supporto della software house Madisoft S.p.A. – proprietaria del Software NUVOLA, le funzionalità del sistema di gestione informatica del protocollo e della gestione documentale affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;

• conservare le copie di salvataggio delle informazioni del sistema e del registro di emergenza in luoghi sicuri differenti;

**ISTITUTO COMPRENSIVO "PERUGIA 14"**
**Codice Meccanografico: PGIC85300B | Codice Fiscale: 94152410547**

Scuola dell'infanzia di Bosco, Montelaguardia, Ponte Felcino e Villa Pitignano
Scuola Primaria di Colombella, Montelaguardia, Ponte Felcino e Villa Pitignano
Scuola Secondaria di I° grado "Bonazzi - Lilli"

• garantire 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 esterno e le attività di gestione degli archivi, quali, trasferimento dei documenti all'archivio di deposito, disposizioni per la conservazione degli archivi e Archivi storici;

• autorizzare le operazioni di annullamento della registratura di protocollo;

• vigilare sull'osservanza delle disposizioni delle norme correnti da parte del personale autorizzato e degli incaricati.

2. di nominare se stessa quale vicario del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, per i casi di vacanza, assenza o impedimento del Responsabile

3. Per lo svolgimento di detto incarico sarà corrisposto un compenso forfettario per non meno di 20 ore (venti) da definirsi in sede di Contrattazione d'Istituto. Il pagamento dell'incarico è subordinato alla presentazione di una relazione finale sull'attività svolta.

**Dirigente Scolastico**
Prof.ssa Marta Boriosi

Per accettazione

_____

# RICHIESTA DI EROGAZIONE SERVIZI DOCFLY CLIENTE PARTNER

Il/La sottoscritto/a, Nome MARTA Cognome BORIOSI C.F. BRSMRT67R71C745L nato/a il 31 / 10 / 1967 a CITTÀ DI CASTELLO Pr. ( PG ), Nazionalità ITALIANA Indirizzo E-Mail* MARTA.BORIOSI@ISTRUZIONE.IT nella sua qualità di titolare/Legale rappresentante della ISTITUTO COMPRENSIVO "PERUGIA 14" con sede in PERUGIA, VIA DELLA TROTA, 12 - CAP 06134 C.F. 94152410547 P.IVA ---------- in ragione del contratto di fornitura dei **Servizi DocFly** concluso con il PARTNER di Aruba Pec S.p.A. MADISOFT, con la sottoscrizione del presente atto, nella sua qualità di CLIENTE PARTNER

**CHIEDE**

alla società Aruba Pec S.p.A l'erogazione dei **Servizi DocFly** come previsti dal suddetto contratto di fornitura.

A tal proposito

**DICHIARA**

**di essere munito dei necessari poteri per impegnare la ditta/società/ente quivi indicato come Cliente Partner sottoscrivendo il presente atto ed i relativi allegati**

**e**

**di accettare integralmente, sempre con la sottoscrizione della presente richiesta dopo averne presa espressa ed attenta visione,**

le Condizioni di Erogazione dei Servizi DocFly Cliente Partner versione 2.0 con gli altri documenti ivi richiamati e quindi in dettaglio:

- Scheda Prodotto DocFly – Conservazione , cliente Partner – versione 2.1;
- Manuale – versione 1.0;
- Policy privacy Aruba Pec S.p.A. – disponibile al link http://www.pec.it/Policy_Privacy.aspx;
- Scheda di conservazione;
- Elenco Persone;
- Nomina Responsabile esterno trattamento dati.

La suddetta documentazione forma e disciplina il "Contratto" avente ad oggetto l'erogazione dei Sevizi DocFly Clienti Partner.

Luogo PERUGIA, data 25 GENNAIO 2016

Il Cliente Partner (Timbro e Firma)

Gruppo Aruba

Ai sensi e per gli effetti degli art. 1341 e 1342 c.c., il Sottoscritto dichiara di aver preso chiara ed esatta visione e di approvare espressamente ed in modo specifico le seguenti clausole delle **Condizioni di Erogazione dei Servizi DocFly Clienti Partner**: 2); 3); 4); 5); 6); 7); 8); 9); 10); 11); 12); 13); 16); 17); 18); 20)

Luogo PERUGIA, data 25 GENNAIO 2016 _____

Il Cliente Partner (Timbro e Firma)

Fermo quanto sopra ai fini dell'erogazione dei Sevizi DocFly, il sottoscritto nella sua qualità di titolare/legale rappresentante del Cliente Partner, tra quelli sopra menzionati, compila, sottoscrive e consegna al Partner, affinché li consegni ad Aruba Pec S.p.A come previsto dal Contratto, i seguenti documenti:

- Scheda di conservazione;
- Elenco Persone;
- Nomina Responsabile esterno trattamento dati;

Luogo PERUGIA, data 25 GENNAIO 2016 _____

Il Cliente Partner (Timbro e Firma)

Sempre ai fini dell'erogazione dei Servizi DocFly avvalendosi delle facoltà previste dal Contratto, il sottoscritto nella sua qualità di titolare/legale rappresentante del Cliente Partner nonché **Responsabile della conservazione**

**NOMINA E DELEGA**

La società **ARUBA PEC S.P.A.**, società a socio unico, in appresso denominata anche "ARUBA PEC", con sede legale in Arezzo (AR), Via Sergio Ramelli, n. 8, assegnataria del codice fiscale e numero di iscrizione al Registro delle Imprese di Arezzo: 01879020517, indirizzo e-mail - conservazione@arubapec.it , nr. Telefono: 0575-050036 nr. Fax: 39 0575 862000,

**"Responsabile del servizio di conservazione"** dei documenti informatici della tipologia riportata nelle Schede di conservazione allegato al Contratto, secondo quanto ivi previsto.

## 1. Funzioni ed attività oggetto della presente delega

**1.1** In forza della presente nomina, ARUBA PEC viene formalmente delegata dal Cliente Partner a svolgere le seguenti attività:

a) definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente, inclusa la gestione delle convenzioni, la definizione degli aspetti tecnico-operativi nonché le modalità di trasferimento da parte del Cliente Partner dei documenti informatici versati in conservazione;

b) gestire il processo di conservazione garantendo nel tempo la conformità alla normativa vigente;

c) generare il rapporto di versamento, secondo le modalità previste dal Manuale;

d) generare e sottoscrivere il pacchetto di distribuzione con Firma digitale nei casi previsti dal Manuale;

e) effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;

f) assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del D.P.C.M.;

j) richiedere la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite; ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute interamente dal Cliente; pertanto, qualora il Cliente Partner non se ne sia fatto carico direttamente, ARUBA PEC è sin da ora autorizzata ad addebitare al Cliente Partner tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza;

k) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti, curare l'aggiornamento periodico del manuale del sistema di conservazione di cui all'art. 8 del D.P.C.M..

**1.2** ARUBA PEC, alla luce di quanto previsto dall'art. 44 del CAD, dovrà verificare che il sistema di conservazione dei documenti informatici garantisca:

- il mantenimento dell'identificazione certa del soggetto che ha formato il documento informatico;
- l'integrità dei documenti informatici depositati in conservazione;
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari, nei modi e nei termini stabiliti nel Manuale;
- il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B, e loro successive modificazioni ed integrazioni.

**1.3** ARUBA PEC dovrà altresì :

- terminare il processo di conservazione dei documenti informatici, entro e non oltre i termini convenuti nell'Elenco dei documenti informatici sottoposti a conservazione allegato al Contratto;
- provvedere, entro i suddetti termini, alla "chiusura" del processo di conservazione, apponendo oltre alla Firma digitale dell'incaricato preposto a tale adempimento, una Marca temporale rilasciata da una Certification Authority iscritta nell'elenco ufficiale dei certificatori tenuto dall'Agenzia per l'Italia Digitale sull'insieme dei documenti ovvero su un'evidenza informatica contenente l'impronta o le impronte dei documenti conservati;
- provvedere, qualora richiesto dal Cliente Partner o dalle Autorità fiscali e normative competenti, all'esibizione dei documenti informatici conservati e delle relative evidenze informatiche che

comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare la loro autenticità e validità giuridica.

Resta inteso che:

a) Aruba PEC non sarà responsabile per la mancata o non corretta esecuzione degli obblighi su di essa incombenti, quale Responsabile del servizio di conservazione in tutti i casi in cui il mancato o non corretto adempimento sia dovuto a cause ad essa non imputabili, quali, a titolo meramente esemplificativo: forza maggiore, calamità naturali, eventi bellici, interventi dell'Autorità;

b) a carico di Aruba PEC non è posto alcun obbligo/dovere di elaborare i documenti informatici versati in conservazione al fine di estrarre i relativi metadati che, pertanto, dovranno essere forniti e associati ai rispettivi documenti esclusivamente a cura e carico del Cliente Partner.

## 2. Deleghe di singole funzioni o fasi del processo

**2.1** ARUBA PEC, quale Responsabile del servizio di conservazione, potrà operare anche attraverso uno o più persone fisiche dalla stessa incaricate all'esecuzione delle attività finalizzate alla conservazione dei documenti informatici nell'ambito della fornitura del Servizio.

**2.2** ARUBA PEC potrà delegare, in tutto o in parte, a terzi soggetti persone fisiche o giuridiche, anche esterne alla propria organizzazione, singole funzioni o fasi del processo di conservazione.

## 3. Corrispettivo

**3.1** Il corrispettivo relativo alla presente nomina è quello regolato e stabilito dal Contratto (art. 3.4 Condizioni)

## 4. Durata

**4.1** La presente nomina di Responsabile del servizio di conservazione avrà la stessa durata del Contratto.

## 5. Comunicazione nuove classi documentali

**5.1** Qualora il Cliente Partner intenda sottoporre a conservazione documenti informatici appartenenti a tipi/classi documentali diverse e/o ulteriori rispetto a quelle indicate nell'Elenco dei documenti informatici sottoposti a conservazione allegato al contratto, dovrà formulare apposita istanza scritta ad ARUBA PEC, allegando ad essa una nuova Scheda di Conservazione dei documenti informatici sottoposti a conservazione.

Luogo PERUGIA, data 25 GENNAIO 2016

Il Cliente Partner (Timbro e Firma)

# NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

in applicazione del "Codice in materia di protezione dei dati personali" ai sensi e per gli effetti degli artt. 4, co. 1, lett. g) e 29 del D.Lgs 30 giugno 2003, n. 196

I.C. "PERUGIA 14", con sede e domicilio fiscale in PERUGIA (PG), Via DELLA TROTA n. 12 ed assegnatario del codice fiscale 94152410547, in persona del DIRIGENTE SCOLASTICO Sig. PROF.SSA MARTA BORIOSI, munito di tutti i necessari poteri per la firma del presente atto, in qualità di Titolare del trattamento, come previsto dal combinato disposto degli artt. 4, co. 1, lett. f) e 28, del D.Lgs 30 giugno 2003, n. 196, di seguito, per brevità, definito "**Titolare del trattamento**";

- visto il Decreto Legislativo 30 giugno 2003, n. 196. *"Codice in materia di protezione dei dati personali"*, di seguito definito *"Codice" e s.m.i.;*

- preso atto che l'art. 4, comma 1, lettera g) del suddetto Decreto definisce qualel "*'responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali";*

- atteso che l'art. 29, commi 2, 3, 4 e 5 del D. Lgs. n. 196/2003 dispone che:
- *"2. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.*
- *3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione dei compiti.*
- *4. I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare.*
- *5. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni";*

- considerato che il compimento di tutti gli atti previsti dal Codice per il trattamento dei dati personali, spettano in via esclusiva al Titolare del trattamento;

- considerato che è stato con Voi stipulato, ed è tuttora in corso di validità, il Contratto per l'erogazione del servizio di conservazione digitale di documenti informatici di cui il Cliente Partner è Titolare e/o Produttore, di seguito per brevità chiamato anche *"Contratto"*, perfezionatosi tra il sottoscritto Titolare del trattamento e la società ARUBA PEC Spa;

- considerato che il perfezionamento del Contratto di cui al punto precedente comporta la necessità di trattare, in nome e per conto del suddetto Titolare, dati personali che, come tali, sono soggetti all'applicazione del Codice in materia di protezione dei dati personali;

**N O M I N A**

La società **ARUBA PEC S.P.A.**, in appresso denominata anche "**ARUBA PEC**", con sede legale in Arezzo (AR), Via Sergio Ramelli, n. 8, assegnataria del codice fiscale e numero di iscrizione al Registro delle Imprese di Arezzo: 01879020517, **RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI**, effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi, per quanto sia strettamente necessario alla corretta esecuzione dei servizi ed al rispetto degli obblighi assunti nel Contratto.

## COMPITI PARTICOLARI DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

Il Responsabile esterno del trattamento, operando nell'ambito dei principi stabiliti dal Codice, deve attenersi ai seguenti **compiti di carattere particolare**:

1. il trattamento dei dati deve essere effettuato solo per le finalità connesse allo svolgimento delle attività oggetto del Contratto, con divieto di qualsiasi altra diversa utilizzazione;
2. deve gestire il sistema informatico, nel quale risiedono i documenti informatici ed i dati del Titolare, in osservanza al disciplinare tecnico di cui all'allegato B) del Codice, attenendosi anche alle disposizioni del Titolare del trattamento in tema di sicurezza;
3. deve predisporre ed aggiornare un sistema di sicurezza informatico idoneo a rispettare le prescrizioni del Codice, adeguandolo anche alle eventuali future norme in materia di sicurezza. Più specificatamente, il Responsabile esterno del trattamento deve:

a) adottare adeguati programmi ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal Codice ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi in conformità allo stesso disciplinare tecnico di cui all'allegato B) del Codice;
b) adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei documenti informatici e dei dati e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura. Il Responsabile esterno del trattamento dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
c) predisporre ed implementare le eventuali ulteriori misure minime di sicurezza imposte dal Disciplinare tecnico di cui all'allegato B) del Codice, per il trattamento informatico dei dati sensibili e per la conseguente tutela degli strumenti elettronici
d) in definitiva, deve adottare adeguate e preventive misure contro i rischi di distruzione o perdita, anche accidentale, dei dati e dei documenti informatici, di accesso non autorizzato e di trattamento non consentito;

4. considerata la complessità delle operazioni tecniche di trattamento ed i compiti assegnati al punto precedente, il Titolare del trattamento autorizza il Responsabile esterno del trattamento ad affidare, sotto la propria responsabilità, l'esecuzione di operazioni di trattamento informatico a soggetti terzi che per connotazione tecnologica, esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto della legge, con particolare riguardo alla sicurezza;
5. può nominare appositi incaricati preposti alle operazioni di trattamento di cui al precedente punto 1); detti incaricati opereranno sotto la diretta autorità del Responsabile esterno del trattamento qui nominato, attenendosi alle istruzioni da questi impartite;
6. deve predisporre e tenere a disposizione, per eventuali verifiche:

a) una breve descrizione del sistema informativo e delle procedure che utilizza per il trattamento dei dati;
b) una descrizione delle misure messe in atto per soddisfare il dettato dell'Allegato B) del Codice, con particolare riferimento all'adozione di adeguate e preventive misure di sicurezza, contro i rischi di distruzione o perdita, anche accidentale, dei dati/documenti informatici stessi, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità connesse allo svolgimento delle attività oggetto del Contratto;
c) la descrizione delle istruzioni impartite agli incaricati;
d) il programma di formazione ed aggiornamento degli incaricati, in materia di privacy e sicurezza:

## PRINCIPI GENERALI DA OSSERVARE A CURA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

7. Ogni trattamento di dati personali deve avvenire, nel rispetto di quanto previsto dal Codice e nel primario rispetto dei principi di ordine generale. In particolare, per ciascun trattamento di propria competenza, il Responsabile esterno del trattamento deve fare in modo che siano sempre rispettati i seguenti presupposti:

a) i dati devono essere trattati:
   - secondo il principio di liceità;
   - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

b) i dati devono, inoltre, essere:
   - trattati soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
   - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento

8. Ciascun trattamento deve avvenire nei limiti imposti dal principio fondamentale di riservatezza e deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
9. Il Responsabile esterno del trattamento è a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni penali (artt. 167 e ss. del Codice).

10. Il Responsabile esterno del trattamento si impegna a non divulgare, diffondere, trasmettere e comunicare i dati/documenti informatici di proprietà del Titolare del trattamento, nella piena consapevolezza che i dati/documenti rimarranno sempre e comunque di proprietà esclusiva dello stesso Titolare del trattamento, e pertanto non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti.
11. Ai sensi e per gli effetti dell'art. 30, co. 5, del Codice, il Titolare del trattamento, ha facoltà di vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza dei compiti e delle istruzioni qui impartite al Responsabile esterno del trattamento.
12. All'atto della conclusione o della revoca dei servizi oggetto del Contratto, il Responsabile esterno del trattamento dovrà consegnare al Titolare del trattamento gli archivi informatici con le modalità previste dal Contratto e dal Manuale del sistema di conservazione e dai documenti ad essi allegati; contestualmente, ARUBA PEC, si impegna a cancellare fisicamente dai propri sistemi e dai propri archivi elettronici tutti i dati/documenti informatici di proprietà del Titolare del trattamento. E' comunque facoltà del Titolare del Trattamento, prelevare in qualsiasi momento gli archivi informatici di sua proprietà usufruendo della specifica funzione prevista dal Contratto e dal Manuale del sistema di conservazione.
13. La presente nomina è condizionata, per oggetto e durata, al Contratto in corso di esecuzione e si intenderà revocata di diritto contestualmente alla cessazione del rapporto medesimo o alla risoluzione, per qualsiasi causa, dello stesso.

Il Titolare del Trattamento nulla più pretenderà rispetto a quanto previsto nel presente atto di nomina e considererà assolto l'adempimento da parte del Responsabile esterno del trattamento con l'applicazione delle procedure sopra indicate.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

**PERUGIA**, lì **25 GENNAIO 2016**

Il Cliente Partner .....
.....

# Scheda conservazione – Registro Giornaliero di protocollo

Elenco dei tipi di documenti informatici che il Cliente Partner intende sottoporre a conservazione utilizzando il Servizio.

| Dati identificativi archivio Cliente | Cognome, nome o ragione sociale | Codice fiscale o partita iva |
|---|---|---|
| | I.C. "PERUGIA 14" | 94152410547 |

| Tab. A - Definizione Documenti | Formati Accettati | Firma digitale |
|---|---|---|
| Registro Giornaliero di protocollo | ☒ PREVISTI DALLA NORMATIVA :PDF - PDF/A, TIFF, JPG, Office Open XML (OOXML) , Open Document Format, XML, TXT, Formati Messaggi di posta elettronica<br>☐ NON PREVISTI DALLA NORMATIVA: 7Z, DATA, MSA, MSG, MSPP, MSWORD, PSD, RTF, XLS, ZIP | FACOLTATIVA |

## METADATI

Elenco metadati obbligatori
Devono essere presenti nell'indice

| TAB. B – METADATI OBBLIGATORI | | |
|---|---|---|
| ID pacchetto di versamento | Denominazione soggetto mittente | Numero ultima registrazione effettuata sul registro |
| IDDocumento **(valore obbligatorio)** | Partita IVA soggetto mittente | Data prima registrazione effettuata sul registro |
| Impronta Documento **(valore obbligatorio)** | Cognome soggetto mittente | Data ultima registrazione effettuata sul registro |
| Data Chiusura | Nome soggetto mittente | Amministrazione titolare del procedimento |
| Oggetto Documento | Codice fiscale soggetto mittente | Amministrazioni partecipanti |
| cognome destinatario | Cognome Soggetto Produttore 2 | Responsabile del procedimento |
| Nome destinatario | Nome Soggetto Produttore 2 | Oggetto del Procedimento |
| Codice Fiscale destinatario | Codice Fiscale Soggetto Produttore 2 | Documenti contenuti nel procedimenti |
| Denominazione destinatario | Cognome Responsabile Gestione Documentale | Numero Protocollo |
| Partita Iva Destinatario | Nome Responsabile Gestione Documentale | Data Registrazione Protocollo |
| Cognome Soggetto Produttore | Codice Fiscale Responsabile Gestione Documentale | AOO di riferimento |
| Nome Soggetto Produttore | Codice identificativo del registro | Codice Identificativo amministrazione (IPA) |
| Partita Iva Soggetto produttore | Numero Progressivo del registro | Denominazione dell'amministrazione |
| Codice Fiscale Soggetto Produttore | Anno | |
| Denominazione Soggetto Produttore | Numero prima registrazione effettuata sul registro | |

Elenco ExtraInfo Disponibili
Non sono obbligatori nell'indice
Possono non essere valorizzati.

| TAB. C – METADATI DISPONIBILI | | |
|---|---|---|
| IDENTIFICAZIONE DEL SISTEMA VERSANTE | DATA DI ALTRA REGISTRAZIONE | IDENTIFICATIVO DELL'UNITÀ ARCHIVISTICA |
| ID DOCUMENTO NEL SISTEMA DI ORIGINE | REGISTRO | ANNOTAZIONE |
| APPLICATIVO DI PRODUZIONE DEL DOCUMENTO | REPERTORIO | ANNESSO |
| LIVELLO DI RISERVATEZZA | SERIE | NOTE 1 |
| CONDIZIONI DI ACCESSO | UFFICIO PRODUTTORE | NOTE 2 |
| CODICE FISCALE TITOLARE DEL CERTIFICATO DI FIRMA | ESISTENZA DI ORIGINALE ANALOGICO | ALLEGATO 1 |
| NUMERO DI ALTRA REGISTRAZIONE | CLASSIFICAZIONE ARCHIVISTICA | ALLEGATO 2 |
| ID FASCICOLO | | |

**NOTE**:
Il Cliente, dopo aver comunicato ad Aruba le caratteristiche, le modalità ed i termini di versamento dei documenti informatici in conservazione, approva espressamente quanto indicato nelle tabelle descrittive sopra riportate, facendole proprie in ogni loro parte, essendo perfettamente coincidenti alle istruzioni dal medesimo impartite.

PERUGIA, lì 25.01.2016

Il Cliente Partner .....



**Madisoft s.r.l.**
Via Falcone, 5 – Casette Verdini
62010 **POLLENZA** - MC
Tel. 0733 203595

Iscrizione. Registro Imprese di Macerata 01818840439
Codice Fiscale e Partita Iva. 01818840439
Capitale Sociale €. 10.000,00 i.v.
http: //scuoladigitale.info
e-mail: info@madisoft.it

# ELENCO PERSONE CLIENTE PARTNER

Di seguito l'elenco delle persone designate dal Cliente Partner ad operare in suo nome, conto e interesse con Aruba Pec per l'esecuzione del contratto in funzione del ruolo:

| **Ruolo** | **Responsabile della Conservazione / Delegato** [1] | **Riceve account e PWD dell'utente master per la gestione del sistema di Riceve tutte le notifiche del processo di conservazione** | |
|---|---|---|---|
| Cognome e Nome incaricato* | BORIOSI MARTA | | |
| Codice Fiscale* | BRSMRT67R71C745L | Luogo e data di nascita* | CITTÀ DI CASTELLO (PG) 31/10/1967 |
| Recapito Tel.* | 075 691131 | Cellulare* | 339 1398850 |
| Indirizzo PEC* | pgic85300b@pec.istruzione.it | Indirizzo e-mail* | conservazione@madisoft.it |

| **Ruolo** | **Responsabile Produttore**[1] | **Riceve tutte le notifiche del processo di conservazione Riceve tutti gli alert amministrativi** | |
|---|---|---|---|
| Selezionare se uguale a | ☒Responsabile della Conservazione / Delegato | | |
| Cognome e Nome incaricato* | | | |
| Codice Fiscale* | | Luogo e data di nascita* | |
| Recapito Tel.[2] | | Cellulare* | |
| Indirizzo PEC [2] | | Indirizzo e-mail [2] | |

| **Ruolo** | **Responsabile Amministrativo** [1] | **Riceve tutti gli alert amministrativi** | |
|---|---|---|---|
| Selezionare se uguale a Produttore | ☐ Responsabile della Conservazione / Delegato | ☐ Responsabile | |
| Cognome e Nome incaricato* | TARDOCCHI GIUSEPPE | | |
| Codice Fiscale* | TRDGPP72C13D786H | Luogo e data di nascita* | UMBERTIDE (PG) IL 13/03/1972 |
| Recapito Tel.[2] | 075 691131 | Cellulare* | 347 9078485 |
| Indirizzo PEC [2] | pgic85300b@pec.istruzione.it | Indirizzo e-mail [2] | giuseppe.tardocchi@istruzione.it |

| **Ruolo** | **Responsabile Tecnico** | **Riceve tutte le notifiche del processo di conservazione Riceve tutti gli alert amministrativi** | |
|---|---|---|---|
| Selezionare se uguale a Produttore | ☐ Responsabile della Conservazione / Delegato | ☐ Responsabile | |
| Cognome e Nome incaricato | TARDOCCHI GIUSEPPE | | |
| Codice Fiscale | TRDGPP72C13D786H | Luogo e data di nascita | UMBERTIDE (PG) IL 13/03/1972 |
| Recapito Tel.[2] | 075 691131 | Cellulare | 347 9078485 |
| Indirizzo PEC [2] | pgic85300b@pec.istruzione.it | Indirizzo e-mail [2] | giuseppe.tardocchi@istruzione.it |

1 Ruolo Obbligatorio – Compilare tutti i campi obbligatori contrassegnati con "*" a meno che non siano uguali ad un ruolo già definito sopra.

2 Campi modificabili anche in caso di riferimento identico ad uno già definito sopra.

Il Cliente Partner dichiara che i suddetti soggetti sono stati dallo stesso valutati come persone esperte ed affidabili ed in grado di interagire autonomamente con Aruba Pec ed il sistema di conservazione alla stessa fornito.
Il Cliente Partner dichiara inoltre di aver impegnato per iscritto i suddetti soggetti a rispettare quanto previsto dal Contratto inclusi i relativi allegati, e che i medesimi a loro volta hanno dichiarato per iscritto di essere informati circa il contenuto dei richiamati documenti e di conoscere quanto previsto dalla Normativa regolante la conservazione di documenti informatici ivi inclusa quella relativa alla privacy. Il Cliente Partner si assume responsabilità in ordine all'operato dei suddetti soggetti impegnandosi a manlevare e/o tenere indenne Aruba Pec da ogni e qualsiasi responsabilità per eventuali richieste danni, diretti o indiretti, da chiunque avanzate per fatti imputabili a detti soggetti.
Il Cliente Partner si obbliga a tenere aggiornato l'elenco dei suddetti incaricati nonché a comunicare tempestivamente ad Aruba ogni variazione rispetto ai dati sopra riportati.

PERUGIA, lì 25.01.2016

Il Cliente Partner .....
.....

# DocFly Conservazione Digitale a Norma – Cliente Partner

## 1. Cosa è

DocFly è un servizio di conservazione digitale, conforme alle disposizioni normative contenute all'interno del DPCM del 3 Dicembre 2013 ed agli standard tecnici espressamente richiamati dallo decreto stesso. La soluzione permette di gestire e conservare a norma qualsiasi tipo di documento informatico, sia in ambito amministrativo che fiscale, rispondendo quindi, con un'unica soluzione a tutte le esigenze di conservazione a norma di legge di ogni realtà produttiva. DocFly assicura, dalla presa in carico fino all'eventuale scarto, la conservazione di documenti e fascicoli informatici, inclusi i metadati associati, garantendo al tempo stesso i requisiti di **autenticità, integrità, affidabilità, leggibilità, reperibilità.**

## 2. Caratteristiche Tecniche

### 2.1 Caratteristiche principali del servizio

DocFly – conservazione digitale a norma, in linea con le disposizioni vigenti, presenta le seguenti caratteristiche:

- salvaguardia dell'integrità dei documenti informatici conservati mediante apposizione della firma digitale;
- prolungamento della validità del documento con apposizione della marca temporale al pacchetto di archiviazione;
- versamento multicanale dei documenti da sottoporre in conservazione;
- accesso diretto tramite interfaccia Web sicura ai documenti informatici conservati,
- totale sicurezza nella trasmissione dei documenti informatici da sottoporre a conservazione;
- completo monitoraggio delle fasi di elaborazione dei documenti;
- gestione degli utenti con possibilità di autorizzare l'accesso solo alle classi documentali di competenza;
- reportistica relativa allo status di utilizzo del servizio DocFly.

Tramite DocFly è possibile conservare correttamente documenti di vario tipo: Amministrativi, a rilevanza tributaria, documenti generici e messaggi PEC.

### 2.2 Formati gestiti

In linea con la normativa vigente il sistema consente la conservazione dei seguenti formati : PDF/PDF-A,TIF, JPG, Office Open XML (OOXML), ODF (Open Document Format), XML, TXT, formati messaggi di posta elettronica .

### 2.3 Metadati

La normativa vigente esplicita i metadati minimi da associare a qualsiasi documento informatico, ovvero, gli indici che devono essere ad esso associati, a prescindere dalla specializzazione che questo assume (amministrativo, fiscale, ecc.).
Oltre a quanto previsto dalla normativa è possibile specificare ulteriori metadati da associare ai documenti quali, ad esempio, il numero delle pagine, l'anno, il periodo d'imposta, ecc.. Tali ulteriori metadati sono oggetto di indicizzazione da parte del sistema ed costituiscono nuove chiavi di interrogazione e ricerca.

### 2.4 Canali di acquisizione dei documenti

I canali di versamento sicuri che il sistema mette a disposizione al fine di ricevere la documentazione soggetta a conservazione sono : web services , ftp , http.

- Web Services: è il canale preferenziale per integrare le applicazioni ed i sistemi del cliente con il sistema di conservazione. Attraverso le interfacce disponibili è possibile sia trasferire documenti sia interrogare il sistema per reperire lo stato dei documenti messi in conservazione.
- FTP/Cartella: tramite questo canale è possibile mediante un client ftp, trasferire i documenti in un'apposita area .. Questa modalità consente upload di un unico file compresso (zip) contenente tutti i file del lotto di conservazione ed è particolarmente indicata per l'inoltro di grosse moli di documenti.
- Http/Online: tramite questo canale è possibile effettuare l'upload dei singoli documenti o dell'intero archivio, tramite pannello web.

### 2.5 Processo di conservazione e condizioni di versamento

La ricezione dei documenti avviene attraverso la costruzione di un pacchetto di versamento (PdV), che contiene oltre ai documenti i metadati ad essi associati (indice), il cui formato deve essere concordato con il conservatore Aruba PEC utilizzando l'apposita Scheda di Conservazione. Fra i diversi aspetti da concordare, i principali sono: le tipologie di documenti da conservare, metadati, eventuali extrainfo, i formati da adottare per ogni classe/tipo documento, le modalità e canali di trasferimento dei documenti nell'archivio (ws, ftp,http) etc. .
L'indice del pacchetto di versamento è un file .xml che contiene le informazioni caratterizzanti il pacchetto stesso quali a titolo esemplificativo ma non esaustivo : id univoco del PdV, id univoco di ogni documento comprensivo della sua impronta e dei metadati che lo descrivono etc etc. .
Il sistema di conservazione, una volta ricevuti i pacchetti di versamento, avvia da subito dei controlli di qualità circa la regolarità di formazione del pacchetto stesso nonché dei dati relativi ai documenti che formeranno oggetto di deposito. I controlli e le notifiche riguardanti le diverse operazioni, che si succedono lungo il processo di conservazione, sono documentate all'interno del manuale del sistema di conservazione.

## 2.6 Gestione e funzionalità del sistema di conservazione

Il servizio e' accessibile tramite interfaccia web. In particolare, e' previsto un pannello di gestione attraverso il quale, l'utente che accede, dispone di tutti gli strumenti utili per la gestione delle sue attività, in linea con i privilegi specifici che sono stati previsti per quella utenza , tra cui:

- Creazione e profilazione utenti: all'attivazione del servizio è prevista la creazione di un account master che consente al cliente di creare e gestire in completa autonomia, uno o più profili, sulla base delle utenze in suo possesso.
- Funzionalità di ricerca e download: tutti i documenti archiviati e conservati possono essere consultati successivamente attraverso le funzionalità di ricerca. L'utente può effettuare il semplice download dei documenti conservati o richiedere la produzione di un pacchetto di distribuzione a norna di legge.
- Gestione dei processi: da pannello l'utente ha la possibilità di visualizzare lo stato reale dei processi di conservazione, incluse notifiche e log relativamente ai documenti versati sul sistema di conservazione.
- Notifiche: le diverse operazioni, che si succedono lungo il processo di conservazione, sono notificate in automatico dal sistema e inviate via mail (PEC) ai riferimenti indicati dal cliente.
- Reportistica: il sistema permette, in tempo reale, di verificare l'utilizzo delle risorse allocate ad uno o più archivi collegati al cliente. Il sistema fornisce uno strumento di reportistica su base mensile, in grado di identificare per il periodo di riferimento scelto, l'allocato e consumato effettivo delle risorse. I report possono essere salvati e recuperati da sistema
- Alert: L'utente riceve degli alert con notifica via mail relativamente alle seguenti informazioni: superamento livelli soglia prestabiliti, rinnovo contrattuale, pagamenti ed altre informazioni relative al contratto.

## 2.7 Modalità di erogazione del servizio e Architettura del sistema

Il servizio DocFly Conservazione Digitale a norma è erogato in modalità outsourcing tramite l'infrastruttura ospitata presso i datacenter del Gruppo Aruba,. rispondono agli elevati standard TIER IV; i dati archiviati sono custoditi al suo interno e i massimi livelli di sicurezza adottati in queste strutture impediscono interruzioni del servizio o tentativi di intrusione e manomissione. la soluzione prevede un'architettura modulare che presenta le seguenti caratteristiche:

- Affidabilità : totale ridondanza ai guasti HW e SW di ogni singolo componente
- Scalabilità : l'architettura è progettata per gestire l'elaborazione di grandi volumi di dati
- Flessibilità : la soluzione è facilmente integrabile e customizzabile
- Storage replicato: il dato posto in conservazione è sempre memorizzato in almeno due infrastrutture storage.

# 3. Caratteristiche generali

| Caratteristiche Generali del Servizio | Specifiche Tecniche |
|---|---|
| **SLA complessivo sul servizio** | 99,95% uptime nel versamento e consultazione |
| **Assistenza** | attraverso il canale trouble ticketing e telefonico |
| **Fasi elaborazione Pacchetti di Versamento** | **Specifiche Tecniche** |
| **Presa in carico del PdV (rapporto di versamento)** | Notifica al cliente entro 48h dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento |
| **Invio in conservazione del PdA (costituiti da uno o più PdV)** | Notifica al cliente entro 96h dal ricevimento dell'ultimo documento |
| **Comunicazioni durante il processo** | **Specifiche Tecniche** |
| **Rapporto di Versamento – PdV Validato** | Notifica entro 4h dalla effettiva presa in carico del PdV |
| **Rapporto di Conservazione – PdV Conservato** | Notifica entro 4h dall'effettiva conservazione del PdV |
| **Richiesta di Esibizione** | **Specifiche Tecniche** |
| **Produzione del Pacchetto di Distribuzione** | Notifica entro 24h dalla richiesta di produzione del PdD |

## 4. Assistenza e canali

E' possibile chiedere assistenza secondo le condizioni concordate con il proprio partner / rivenditore .

# *Ministero dell'Istruzione, dell'Università e della Ricerca*

**ISTITUTO COMPRENSIVO PERUGIA 14**

**Scheda di apertura/chiusura del registro di emergenza**

Causa dell'interruzione: _____

Data inizio evento: ___/____/_____ ___:____ Data fine evento: ___/____/_____ ___:____

Annotazioni: _____

Numero protocollo: iniziale _____ finale _____ Pagine n._____

| DATA REGISTR. | Numero | DIR. (E/U) | TITOLARIO | MITTENTE / DESTINATARIO | OGGETTO |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |



Il compilatore

_____

Il Responsabile del servizio Protocollo

_____

| DATA REGISTR. | Numero | DIR. (E/U) | MITTENTE | MITTENTE/DESTINATARIO | OGGETTO |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Il compilatore

_____

Il Responsabile del servizio Protocollo

_____

# Ministero dell'Istruzione, dell'Università e della Ricerca

**ISTITUTO COMPRENSIVO PERUGIA 14**

**Registro delle richieste di annullamento delle registrazioni di protocollo**

| DATA REGISTR. | Numero | DIR. (E/U) | TITOLARIO | MITTENTE / DESTINATARIO | MOTIVO DELL'ANNULLAMENTO | NUOVO NUMERO DI PROTOCOLLO |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |



Il Responsabile del servizio Protocollo

_____