



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

**Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

### REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

(REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Regolamento 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Articolo 30 - Registri delle attività di trattamento)

**Titolare del trattamento dei dati:** IIS "MINUZIANO – DI SANGRO ALBERTI" SAN SEVERO

Legale rappresentante - Dirigente Scolastico in carica, prof. Vincenzo CAMPAGNA

elettivamente domiciliato presso la Scuola: IIS "Minuziano-Di Sangro Alberti" -mail

istituzionale [fgis0.3700v@istruzione.it](mailto:fgis0.3700v@istruzione.it)

**Responsabile del trattamento dei dati** - DSGA, elettivamente domiciliato presso la Scuola:

Sig.Paolo Michele SILVESTRIS - mail istituzionale [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it)

**Responsabile della protezione dei dati:** Prof.ssa Avv. GRECO MARIA ANTONIETTA –

[greco.mariaantonietta@avvocatifoggia.legalmail.it](mailto:greco.mariaantonietta@avvocatifoggia.legalmail.it)

Supporto al RPD – area di riferimento: dati trattati con mezzi informatici – prof. LUIGI MANZELLA

Supporto al RPD – area di riferimento: dati trattati in cartaceo – Sig.ra Annalisa MORELLI

I dati personali sono trattati tramite gli applicativi informatici "Segreteria Digitale" e altro" forniti da ARGO SOFTWARE srl. Il Gruppo Argo software è il Fornitore dei suddetti servizi e, in quanto tale, tratta i dati personali ai sensi del GDPR, cioè qualora "un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".

**Responsabile Esterno del trattamento dei dati:** prof. Lorenzo LO PRESTI, Rappresentante Legale Argo software srl

#### 1.1 Finalità generali del trattamento

Ai sensi dell'art. 4 del GDPR, i dati personali sono "qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Nel dettaglio, i dati personali trattati dalla scuola *SECONDARIA DI 2 GRADO IIS "MINUZIANO – DI SANGRO ALBERTI" di SAN SEVERO* nonché le finalità dei trattamenti al fine di svolgere i servizi scolastici e amministrativi sono indicati all'interno del Registro dei trattamenti del Titolare, riportato di seguito.

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico, ai sensi degli articoli 20 e 21 del D.lgs 196/2003. Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori.

**Norma di riferimento: Ministero della Pubblica Istruzione Decreto 7 dicembre 2006 n. 305**

#### 1.2 Luoghi di tenuta e trattamento dei dati:

I dati su supporto cartaceo sono conservati negli armadi degli uffici: amministrativo-didattico; amministrativo-contabile; nel locale denominato archivio, sito nel seminterrato dell'edificio della sede Centrale e nell'ufficio amministrativo-didattico di San Severo

I dati su supporto elettronico sono conservati negli archivi elettronici dei computer di tutti i servizi amministrativi.

(Nella tabella che segue, relativamente ai dati sensibili e giudiziari, nella descrizione sintetica del trattamento, le finalità e le attività svolte, i tipi di dati trattati e le operazioni eseguite sono indicati in modo sintetico e con riferimento alle schede allegato al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse, con specificazione, per ogni identificativo di trattamento, delle specifiche schede)



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

### Polo Tecnologico "A. Minuziano – Di Sangro Alberti"

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

### 1.3 Disposizioni per la gestione dei documenti in entrata e in uscita

Tutti i documenti in entrata, sia in formato digitale che cartaceo, contenenti dati sensibili e giudiziari appartenenti a Alunni – Genitori – Personale – Fornitori – Personale esterno – Soggetti terzi devono essere assegnati preventivamente e in via esclusiva al Titolare del trattamento dei dati nella persona del dirigente scolastico.

Il Titolare del trattamento dei dati assegnerà il documento esclusivamente all'assegnatario incaricato e autorizzato del trattamento di quella tipologia di dati per la categoria di interessati con protocollo riservato.

Ogni incaricato del trattamento dei dati disporrà di una casella personale di posta elettronica [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) alla quale il Titolare del trattamento indirizzerà e consegnerà il documento riservato di propria competenza.

Per i documenti in uscita si osserveranno le medesime regole di gestione del protocollo riservato da parte del Titolare e dell'incaricato del trattamento dei dati.

### 2.1 Diritti dell'interessato

In qualunque momento l'interessato potrà esercitare i diritti di cui all'art. 7 del D. Lgs. 196/03, agli artt. 15, 16, 17, 18 del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 Aprile 2016 in merito all'accesso, all'aggiornamento, alla rettifica o integrazione, alla limitazione, diritto di presentare un reclamo all'autorità di controllo, alla cancellazione dei dati personali registrati, quale diritto all'oblio, e alla revoca del consenso. A seguito della revoca del consenso, vi sarà la cancellazione dei dati e la conseguente impossibilità di fornire ulteriori servizi.

Le eventuali comunicazioni dovranno essere inviate al Titolare del trattamento tramite la Segreteria: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it)

### 2.2 Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti qualora il trattamento sia effettuato con mezzi automatizzati. Ha, altresì, il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

### 3.1 Violazione dei Dati Personali

Il Titolare del Trattamento si impegna a comunicare per iscritto all'interessato, tempestivamente ogni violazione dei Dati Personali che riguardi o afferisca ai Trattamenti dei Dati Personali eseguiti dallo stesso Titolare o dal Fornitore esterno dei servizi o da qualsivoglia Sub- responsabile.

### 3.2 Trasferimento dei Dati Personali

Salvo un espresso consenso rilasciato per iscritto dall'interessato, il Titolare del trattamento non trasferisce, né direttamente né per il tramite di soggetti terzi, i Dati Personali verso paesi non aderenti all'Unione Europea o organizzazioni internazionali

### 4.1 Termini ultimi previsti per la cancellazione delle diverse categorie di dati

Norma di riferimento: Ministero della Pubblica Istruzione Ufficio Scolastico Regionale per la PUGLIA Direzione Generale Massimario di scarto e conservazione in Allegato su sito web:

<http://www.polotecnologico-sansevero.gov.it/amministrazione-trasparente/altri-contenuti/>

Terminato il trattamento utile all'erogazione e all'espletamento dei servizi, i dati verranno anonimizzati

## 5. DATI PERSONALI

### 5.1 Anagrafica dello studente:

Nome	Cognome	Luogo di nascita	Data di nascita	Cittadinanza
Seconda Cittadinanza	Sesso	Codice Fiscale	Residenza	Recapito
Telefono	Cellulare	Email	Pec (non utilizzata)	Email 2
Skype (non utilizzata)	Matricola (non utilizzata)	Codice Alunno Sidi	Dati Sogei (non utilizzati)	Fotografia (non utilizzata)

### 5.2 Anagrafica degli esercenti la potestà genitoriale:

Nome	Cognome	Luogo di nascita	Data di nascita	Cittadinanza
Seconda Cittadinanza	Sesso	Codice Fiscale	Ruolo	Residenza
Recapito	Telefono	Cellulare	Email	Pec
Email 2	Skype (non utilizzata)	Stato civile	Titolo di studio	Professione

### 5.3 Altri dati dello studente:

Curriculum scolastico  
Crediti  
Piano studi  
Permessi autorizzati

**ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO****Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

Documenti

Vaccinazioni

Rette – Tasse scolastiche – Esenzioni - Fiscalità

Voti, valutazioni, giudizi, annotazioni, provvedimenti, autorizzazioni

**Tipologie di trattamenti:**

Raccolta	Presso gli interessati	X	Presso terzi	X
Elaborazione	Forma cartacea	X	Modalità informatizzate	X

Altre	Registrazione – organizzazione – Conservazione – Consultazione – Modificazione – Selezione, Estrazione – Utilizzo – Blocco – Cancellazione - distruzione
-------	--

In allegato l'elenco degli uffici incaricati del trattamento dei dati con le rispettive abilitazioni e permessi.

**Tabella 1 – Elenco dei trattamenti dei dati (specifiche in tabelle singole)**

Descrizione sintetica del Trattamento		Natura dei dati trattati S – G	Struttura di riferimento	Terzi da cui provengono i dati e a cui vengono comunicati i dati
Finalità perseguita o attività svolta	Categorie di interessati			
<b>Gestione Area Alunni</b> Relativamente ai dati sensibili e giudiziari : Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico; Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	Alunni – Genitori	S – G	Segreteria didattica Dirigente Scolastico	USR, UST, MIUR, Altre istituzioni scolastiche, ASL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, altri soggetti pubblici o privati per percorsi formativi, di assistenza, di orientamento, Avvocature dello Stato, Magistrature ordinarie, Organi di polizia giudiziaria, Liberi professionisti (avvocati), Polizia Municipale
Gestione Provvedimenti Disciplinari alunni Relativamente ai dati sensibili e giudiziari : Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico; Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	<i>Genitori, Alunni, Personale</i>	S – G	Segreteria didattica Dirigente Scolastico	Genitori, UST, USR, Servizi Sociali, Autorità di Polizia, Procura della Repubblica e Procura dei Minori

**a) nelle attività propedeutiche all'avvio dell'anno scolastico:**

- dati relativi alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana;
- dati relativi alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- dati relativi allo stato di salute, per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi;
- dati relativi alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione (i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti degli alunni che abbiano commesso reati).



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

**Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

### b) nell'espletamento dell'attività educativa, didattica, formativa e di valutazione:

- dati relativi alle origini razziali ed etniche per favorire l'integrazione degli alunni con cittadinanza non italiana;
- dati relativi alle convinzioni religiose per garantire la libertà di credo religioso; dati relativi allo stato di salute, per assicurare l'erogazione dei servizi di enti locali, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;
- dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- dati relativi alle convinzioni politiche, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori.

### c) nella gestione del contenzioso nel rapporto scuola - famiglie - alunni:

dati sensibili e giudiziari concernenti tutte le attività connesse alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali

**Finalità di rilevante interesse pubblico perseguite:** artt. 67, 68, 71, 73, 86, 95 del D.Lgs. 30 giugno, n. 196

**Fonti normative:** leggi regionali sul diritto allo studio ai sensi del DPR 24 luglio 1977 n. 616; L. 25 marzo 1985, n. 121; L. 5 febbraio 1992, n. 104; D.Lgs. 16 aprile 1994, n. 297; DPR 10 ottobre 1996, n. 567; L. 24 giugno 1997, n. 196; D.Lgs. 31 marzo 1998, n. 112; DPR 24 giugno 1998, n.249; DPR 8 marzo 1999, n. 275; DPR 31 agosto 1999, n. 394; L. 10 marzo 2000, n. 62; L. 28 marzo 2003, n. 53; D.Lgs. 19 febbraio 2004, n. 59; D.Lgs. 15 aprile 2005, n. 76; D.Lgs. 15 aprile 2005, n. 77; D.Lgs. 17 ottobre 2005, n. 226; L. 170/2010; BES-Dir. Min. 27/12/2012; C.M. n. 8 del 6/03/2013; L. 107/2015 e Decr. Attuativi; Codice Civile; Codice Penale; DPR 24 novembre 1991, n. 1199.

### Tipi di dati trattati:

Origine	Razziale	X	Etnica	X		
Convinzioni	Religiose	X	Filosofiche	X	Altro genere	X
	Politiche	X	Sindacali			
Stato di salute	Patologie attuali	X	Patologie pregresse	X		
	Terapie in corso	X	Dati sulla salute relativi ai familiari	X		
Vita sessuale		X				
Giudiziari	(art. 4, comma 1, lett.e del Codice	X				

### Operazioni eseguite e specifiche forme di trattamento:

Comunicazione ai seguenti soggetti per le seguenti finalità

A – Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 31 marzo 1998, n. 112, con limitazioni ai dati indispensabili all'erogazione del servizio;

B – Gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio ai sensi del DPR 24 luglio 1977 n. 616 con limitazioni ai dati indispensabili all'erogazione del servizio;

C – AA.SS.LL. e Enti Locali per il funzionamento dei gruppi di lavoro per l'inclusione e per la predisposizione dei P.E.I. e dei P.D.P., ai sensi della L. 5 febbraio 1992, n. 104, della L. 170/2010 e BES-Dir. Min. 27/12/2012; C.M. n. 8 del 6/03/2013;

D – Istituzioni scolastiche statali e non statali per la documentazione sulla carriera scolastica con limitazioni ai dati indispensabili all'erogazione del servizio;

E – Istituti di assicurazione per denunce di infortuni e responsabilità civile con limitazioni ai dati indispensabili all'erogazione del servizio;

F – Aziende, imprese, soggetti pubblici e privati per stage, alternanza scuola lavoro, attività di rilevante interesse sociale con limitazioni ai dati indispensabili all'erogazione del servizio;

G – Avvocatura dello Stato per difesa erariale e consulenza

H – Magistrature ordinarie e amministrativo-contabile, Polizia Municipale e Organi di Polizia giudiziaria per l'esercizio dell'esercizio delle funzioni

I – Liberi professionisti, per patrocinio o consulenza compresi le controparti ai fini della corrispondenza

### Altre tipologie di trattamenti:

Raccolta	Presso gli interessati	X	Presso terzi	X
Elaborazione	Forma cartacea	X	Modalità informatizzate	X

Altre	Registrazione – organizzazione – Conservazione – Consultazione – Modificazione – Selezione, Estrazione – Raffronto – Utilizzo – Blocco – Cancellazione - distruzione
-------	--

**ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO****Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V****Termini ultimi previsti per la cancellazione delle diverse categorie di dati**

Norma di riferimento: Ministero della Pubblica Istruzione Ufficio Scolastico Regionale per la PUGLIA Direzione Generale

**Massimario di scarto e conservazione in Allegato su sito web:**<http://www.la.scuola.gov.it/amministrazione-trasparente/altri-contenuti/>

Terminato il trattamento utile all'erogazione e all'espletamento dei servizi, i dati verranno anonimizzati

Gestione Area Bilancio	Personale Fornitori		Segreteria amministrativa	UST, USR, MIUR, Agenzia delle Entrate, Altre istituzioni scolastiche, INPDAP, INPS, INAIL, ASL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Banca servizio di cassa
------------------------	---------------------	--	---------------------------	--

**a) Relativamente a specifiche procedure negoziali definite dal Codice dei contratti pubblici Decreto legislativo 18 aprile 2016, n. 50, dal D. 44/2001:**

- A: Esclusione per motivi legati a condanne penali  
 b: Esclusione per motivi legati al pagamento di imposte o contributi previdenziali  
 c: Esclusione per motivi legati a insolvenza, conflitto di interessi o illeciti professionali  
 d: Capacità economica e finanziaria

**b) Sanzioni interdittive, violazioni e omissioni****c) Relativamente alla gestione del contenzioso:**

dati sensibili e giudiziari concernenti tutte le attività relative alla difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

**Finalità di rilevante interesse pubblico perseguite:** artt. 67, 68, 70, 72, 73, 95, 112 del D.Lgs. 30 giugno, n. 196**Fonti normative:**

Codice Civile; Codice Penale; Codice di procedura Civile; Codice di procedura Penale; Codice dei contratti pubblici Decreto legislativo 18 aprile 2016, n. 50; D. 44/2001; Delibere ANAC, in particolare delibera n. 72/2013; L. 6 novembre 2012, n. 190; decreto MIUR prot. n. 542 del 30 giugno 2016; DPR 16 aprile 2013, n. 62; D.Lgs. 9 aprile 2008, n. 81

**Tipi di dati trattati:**

Giudiziari	(art. 4, comma 1, lett.e del Codice	X	Fiscali	X	
------------	-------------------------------------	---	---------	---	--

**Operazioni eseguite e specifiche forme di trattamento:**

Interconnessioni e raffronti di dati con altro titolare

Comunicazione ai seguenti soggetti per le seguenti finalità

- Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;
- Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (D.lgs. n. 626/1994)
- Organi di controllo (Corte dei Conti e MEF)
- Agenzia delle Entrate: ai fini degli obblighi fiscali;
- UST, USR, MIUR, Altre istituzioni scolastiche;
- INPS, INAIL, ASL, Altre Amministrazioni Pubbliche;
- EQUITALIA, ANAC, AVCP, Banca servizio di cassa
- Alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
- Alle Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;
- Ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.

**Altre tipologie di trattamenti:**

Raccolta	Presso gli interessati	X	Presso terzi	X
Elaborazione	Forma cartacea	X	Modalità informatizzate	X

Altre	Registrazione – organizzazione – Conservazione – Consultazione – Modificazione – Selezione, Estrazione – Utilizzo – Blocco – Cancellazione - distruzione
-------	--

Gestione Area Personale Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e	Personale docente e A.T.A.	S – G	Dirigente Scolastico Segreteria amministrativa	UST, USR, MIUR, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, INPDAP, INPS,
--	----------------------------	-------	--	---



**ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO**

**Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

reclutamento a TI e TD e gestione del rapporto di lavoro; Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari; Scheda n. 3 – Organismi collegiali e commissioni istituzionali; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.				INAIL, ASL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Centro per l'impiego
Gestione Area Retribuzioni Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari; Scheda n. 3 – Organismi collegiali e commissioni istituzionali;	Personale docente e A.T.A.	S – G	Dirigente Scolastico Segreteria amministrativa	UST, USR, MIUR, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, INPDAP, INPS, INAIL, ASL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Magistrature ordinarie e amministrativo-contabile, Agenzia delle Entrate, Banca che effettua il servizio di cassa
Gestione Fiscale	Personale docente e A.T.A.		Segreteria amministrativa	UST, MIUR, Agenzia delle Entrate, Corte dei Conti, Enti assistenziali, previdenziali e assicurativi, MEF, Banca che effettua il servizio di cassa

**a) Relativamente alle operazioni di selezioni di reclutamento indeterminato e determinato e alla gestione del rapporto di lavoro anche diverso da quello subordinato:**

- ◆ dati inerenti lo stato di salute trattati per l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c. d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatorie e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;
- ◆ dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;
- ◆ dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione;
- ◆ dati sulle convinzioni filosofiche o d'altro genere che possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;
- ◆ dati di carattere giudiziario trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato;
- ◆ informazioni sulla vita sessuale che possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso;

**b) Relativamente alla gestione del contenzioso e dei procedimenti disciplinari:**

- ◆ dati sensibili e giudiziari concernenti tutte le attività relative alla difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

**c) Relativamente al funzionamento degli Organismi collegiali e delle commissioni istituzionali:**



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

**Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

- ♦ dati sensibili (appartenenza alle organizzazioni sindacali) necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico.

d) Relativamente alla gestione del contenzioso tra la scuola e le famiglie degli alunni:

dati sensibili e giudiziari concernenti tutte le attività connesse alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

**Finalità di rilevante interesse pubblico perseguite:** artt. 62, 65, 67, 68, 70, 72, 73, 95, 112 del D.Lgs. 30 giugno, n. 196

**Fonti normative:** DPR 10 gennaio 1957, L. 5 febbraio 1992, n. 104; n.3; L. 12 marzo 1999, n. 68; D.Lgs. 30 marzo 2001, n. 165; L. 15 luglio 2002, n. 145; R.D. 30 settembre 1922, n. 1290; L. 24 maggio 1970, n. 336; L. 30 dicembre 1971, n. 1204; DPR 29 dicembre 1973, n. 1092; L. 7 febbraio 1979, n. 29; L. 5 marzo 1990, n. 45; D.Lgs. 30 dicembre 1992, n. 503; L. 14 gennaio 1994, n. 20; L. 8 agosto 1995, n. 135; DPR 20 febbraio 1998, n. 38; L. 12 marzo 1999, n. 68; DPCM 20 dicembre 1999; L. 8 marzo 2000, n. 53; DPR 29 ottobre 2001, n. 461; L. 3 marzo 1999, n. 124; D.Lgs. 16 aprile 1994, n. 297; L. 28 marzo 2003, n. 53; L. 18 luglio 2003, n. 186; D.Lgs. 19 febbraio 2004, n. 59; L. 6 giugno 2004, n. 143 Contratti Collettivi nazionali e integrativi del Comparto Istruzione e Ricerca; L. 28 febbraio 1990, n. 37; L. 23 dicembre 1998, n. 448; DPR 6 marzo 2001, n. 190; L. 27 dicembre 2002, n. 289; D.Lgs. 17 ottobre 2005, n.227.

Codice Civile; Codice Penale; Codice di procedura Civile; Codice di procedura Penale:

### Tipi di dati trattati:

Origini	Razziale	X	Etnica	X		
Convinzioni	Religiose	X	Filosofiche	X	Altro genere	X
	Politiche	X	Sindacali	X		
Stato di salute	Patologie attuali	X	Patologie pregresse	X		
	Terapie in corso	X	Dati sulla salute relativi ai familiari	X		
Vita sessuale		X				
Giudiziari	(art. 4, comma 1, lett.e del Codice	X				

### Operazioni eseguite e specifiche forme di trattamento:

Interconnessioni e raffronti di dati con altro titolare

Comunicazione ai seguenti soggetti per le seguenti finalità

- o Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;
- o Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
- o Organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001;
- o Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (D.lgs. n. 626/1994)
- o Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del D.P.R. n. 1124/1965;
- o Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999;
- o Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- o Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- o Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186;
- o Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e D.P.R. 20 febbraio 1998, n.38;
- o Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;
- o MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335;
- o Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, D.lgs. n. 165/2001).
- o Alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
- o Alle Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;
- o Ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.

### Altre tipologie di trattamenti:

Raccolta	Presso gli interessati	X	Presso terzi	X
----------	------------------------	---	--------------	---

**ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO****Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

Elaborazione	Forma cartacea	X	Modalità informatizzate	X
--------------	----------------	---	-------------------------	---

Altre	Registrazione – organizzazione – Conservazione – Consultazione – Modificazione – Selezione, Estrazione – Utilizzo – Blocco – Cancellazione - distruzione
-------	--

Gestione Protocollo Relativamente ai dati sensibili e giudiziari: Tutte le schede allegato al regolamento sul trattamento dei dati sensibili e giudiziari	Alunni, Genitori, Fornitori, Personale, Altre amministrazioni	S – G	Dirigente Scolastico Segreteria Ammin.va Segreteria Didattica	UST, USR, MIUR, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, INPDAP, INPS, INAIL, ASL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Banca che effettua il servizio di cassa
Gestione Sicurezza	Personale amministrativo accesso aree ----- -----		Segreteria amministrativa	
Backup e Restore	Banca dati Amministrativa		Segreteria amministrativa	
Gestione Protocollo e corrispondenza riservata Relativamente ai dati sensibili e giudiziari: Tutte le schede allegato al regolamento sul trattamento dei dati sensibili e giudiziari	Alunni, genitori, personale	S – G	Dirigente Scolastico	UST, MIUR, Altre istituzioni scolastiche, ASL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola lavoro, Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Organi di polizia giudiziaria, Liberi professionisti
Gestione della posta elettronica	Personale, utenti del servizio scolastico, fornitori		Segreteria amministrativa	
Gestione Scioperi del Personale dipendente Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;	Personale	S	Segreteria amministrativa	<a href="https://websptnet.tesoro.it/SCIOPNET">https://websptnet.tesoro.it/SCIOPNET</a>
Gestione Anagrafe delle prestazioni	Personale interno ed esterno, Fornitori		Segreteria amministrativa	<a href="http://www.anagrafeprestazioni.it">www.anagrafeprestazioni.it</a> Piattaforma SIDI Piattaforma NoiPa
Invio documenti tramite Entratel	Personale esterno e della scuola		Segreteria amministrativa	Sito entrate

**ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO****Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

Gestione INPS - Uniemens	Personale	S	Segreteria amministrativa	Sito inps
Gestione con Suite Microsoft Office comunicazione	Personale interno ed esterno, Fornitori		Segreteria Amministrativa Segreteria Didattica	
Gestione Dispositivi dell'infrastruttura tecnologica	Personale interno ed esterno, Fornitori		Segreteria Amministrativa Segreteria Didattica	
Gestione Graduatorie e supplenze	Personale		Segreteria Amministrativa	UST, USR, MIUR
Gestione del personale	Personale	S - G	Segreteria Amministrativa	Piattaforma SIDI Piattaforma NoiPa
Gestione offerta formativa e Contratti prestazione	Personale interno ed esterno Alunni		Dirigente Scolastico Segreteria Amministrativa	Enti Pubblici Territoriali, INAIL, Organizzazioni Sindacali, Associazioni e Ditte Esterne
Gestione Trattative sindacali Relativamente ai dati sensibili e giudiziari : Scheda n. 3 – Organismi collegiali e commissioni istituzionali;	Contrattazione sindacale	S	Dirigente Scolastico	Componenti RSU Organizzazioni Sindacali
Gestione Archivio cartaceo storico	Tutte le categorie	S - G	Segreteria Amministrativa	I dati non vengono comunicati a terzi (prima dell'eventuale comunicazione vengono trasferiti alle strutture interne autorizzate al trattamento)
Gestione Assistenza e manutenzione hardware	Tutti i soggetti che utilizzano i PC degli uffici Amministrativi		Segreteria Amministrativa	
Gestione titolare Generale			Segreteria Amministrativa	UST, USR, MIUR
Gestione Riproduzione e notifica documenti	Personale, Alunni, Genitori Fornitori		Segreteria Amministrativa	
Gestione Atti cartacei amministrativi	Personale, Alunni, Genitori Fornitori		Segreteria Amministrativa	
Gestione Inventario e Fornitori di beni e servizi	Ditte esterne		Segreteria Amministrativa	Ditte esterne

**3. Descrizione generale delle misure di sicurezza tecniche e organizzative****MISURE DI CARATTERE ELETTRONICO/INFORMATICO**Le misure di carattere elettronico/informatico<sup>1</sup> adottate sono:

- utilizzo di server con configurazioni di ridondanza: la misura è attiva;
- presenza di gruppi di continuità elettrica per il server: la misura è attiva;
- attivazione di un sistema di backup centralizzato non automatizzato con periodicità settimanale e storico di

<sup>1</sup> Le misure di carattere elettronico/informatico sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

**Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

un mese: la misura è attiva. Alla data di questo documento i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati;

- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet: la misura è attiva;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 e XP, Win 8, Win 8.1, Win 10 Pro, Win 7 Pro, di seguito specificate: la misura è attiva;
- installazione di un sistema antivirus su tutti le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria: la misura è attiva;
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate;
- separazione della rete locale delle segreterie da quella dei laboratori didattici: la misura è attiva.

### REGOLE PER LA GESTIONE DELLE PASSWORD<sup>2</sup>

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato user-id) e password personale.

User-id e password iniziali sono assegnati, dal custode delle password.

User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

L'user-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.

La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.

Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema in veste anche di custode delle password, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.

Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

- le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
- per la definizione/gestione della password devono essere rispettate le seguenti regole:
  - la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
  - deve contenere almeno un carattere alfabetico ed uno numerico;
  - non deve contenere più di due caratteri identici consecutivi;
  - non deve contenere lo user-id come parte della password;
  - al primo accesso la password ottenuta dal custode delle password deve essere cambiata; la nuova password non deve essere simile alla password precedente;
  - la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
  - la password termina dopo sei mesi di inattività;
  - la password è segreta e non deve essere comunicata ad altri;
  - la password va custodita con diligenza e riservatezza;
  - l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

<sup>2</sup> La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

### **Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

---

### **REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO**

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su HD e Server si riferiscono al PC dominio associato al PC Server. Esse sono conservate nella cassaforte ubicata nell'ufficio della Segreteria amministrativa
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Il fax si trova in locale ad accesso controllato, l'ufficio della Segreteria didattica e l'utilizzo è consentito unicamente agli incaricati del trattamento dei dati.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiara per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

### **REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS**

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- disattivare gli Activex e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- non attivare le condivisioni dell'HD in scrittura.



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

### Polo Tecnologico "A. Minuziano – Di Sangro Alberti"

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

1. formattare l'Hard Disk, definire le partizioni e reinstallare il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
2. installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
3. reinstallare i programmi applicativi a partire dai supporti originali;
4. effettuare il RESTORE dei soli dati a partire da una copia di backup recente. **NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;**
5. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
6. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

### INCIDENT RESPONSE E RIPRISTINO

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente (vedi tabella 3). **Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso<sup>3</sup>;**
4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

1. eseguire una copia bit to bit degli hard disk del sistema compromesso;

<sup>3</sup> E' indispensabile che per una eventuale indagine venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

### Polo Tecnologico "A. Minuziano – Di Sangro Alberti"

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

2. se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
3. se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

**Tabella 3 - Procedure di spegnimento**

Sistema operativo	Azione
Windows 2000 e XP, Win 8, Win 8.1, Win 10 Pro, Win 7 Pro	<ol style="list-style-type: none"> <li>1. Fotografare lo schermo e documentare i programmi che sono attivi.</li> <li>2. Staccare la spina dalla presa di corrente.</li> </ol>

Nota: (fonte U.S. Departement of Energy)

## UTILIZZO DELLE RETI

### Articolo 1

#### OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica della scuola SECONDARIA DI II GRADO IIS "Minuziano –Di Sangro Alberti" di SAN SEVERO e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire. La rete dell'istituto è connessa alla rete Internet.

### Articolo 2

#### PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

La scuola SECONDARIA 2 GRADO IIS "MINUZIANO-DI SANGRO ALBERTI" di SAN SEVERO promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.

Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

### Articolo 3

#### ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso<sup>4</sup>. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale della scuola
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella dell'istituto;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne

<sup>4</sup> Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale.



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

### **Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

restringano l'utilizzabilità e le prestazioni per altri utenti;

- agire deliberatamente con attività che distruggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica dell'istituto per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

#### **Articolo 4 ATTIVITÀ CONSENTITE**

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

#### **Articolo 5 SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE**

Hanno diritto ad accedere alla rete della scuola SECONDARIA DI 2 GRADO IIS "Minuziano – Di Sangro Alberti" di San Severo tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.

L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

### **Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

#### **Articolo 6**

#### **MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI**

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.

Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

#### **Articolo 7**

#### **SANZIONI**

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti dell'istituto.

#### **MINACCE A CUI SONO SOTTOPOSTE LE RISORSE HARDWARE**

Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;
- malfunzionamenti dovuti a sabotaggi, furti, intercettazioni (appareati di comunicazione).

#### **MINACCE A CUI SONO SOTTOPOSTE LE RISORSE CONNESSE IN RETE**

Le principali minacce alle risorse connesse in rete possono provenire dall'interno dell'istituto, dall'esterno o da una combinazione interno/esterno e sono relative:

- all'utilizzo della LAN/Intranet (interne);
- ai punti di contatto con il mondo esterno attraverso Internet (esterne);
- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:

#### **IP SPOOFING**

L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

#### **PACKET SNIFFING**

Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso è possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

#### **PORT SCANNING**

Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

#### **HIGHJACKING**

Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che



## ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO

### Polo Tecnologico "A. Minuziano – Di Sangro Alberti"

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione è complessa e richiede elevate capacità e rapidità d'azione.

#### **SOCIAL ENGINEERING**

Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

#### **BUFFER OVERFLOW**

Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

#### **SPAMMING**

Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

#### **PASSWORD CRACKING**

Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

#### **TROJAN**

Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsapevolmente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

#### **WORM**

Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

#### **CRIPTOLOCKER**

Questo virus è una forma di ransomware infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione. CryptoLocker generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da istituzioni legittime, o viene caricato su un computer già facente parte di una botnet. Un file ZIP allegato alla e-mail contiene un file eseguibile con una icona e una estensione pdf, avvalendosi del fatto che i recenti sistemi Windows non mostrano di default le estensioni dei file (un file chiamato nomefile.pdf.exe sarà mostrato come nomefile.pdf nonostante sia un eseguibile). Alcune varianti del malware possono invece contenere il Trojan Zeus, che a sua volta, installa CryptoLocker.

#### **LOGIC BOMB**

Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

#### **MALWARE E MMC (MALICIOUS MOBILE CODE)**

Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

#### **DOS (DENIAL OF SERVICE)**

Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

#### **DDOS (DISTRIBUTED DENIAL OF SERVICE)**

Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete

L'utilizzo di programmi di sniffing e port scanning è riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete della scuola SECONDARIA DI 2 GRADO IIS "Minuziano- Di Sangro Alberti di San Severo; tali programmi non sono in nessun caso utilizzati su reti esterne a quella dell'istituto. La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

#### **MINACCE A CUI SONO SOTTOPOSTI I DATI TRATTATI**

Le principali minacce ai dati trattati sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.



**ISTITUTO D'ISTRUZIONE SECONDARIA DI 2° GRADO**

**Polo Tecnologico "A. Minuziano – Di Sangro Alberti"**

con convitto annesso all'ITAS

Via Vincenzo Alfieri, 1 – 71016 San Severo (Fg) - Italia

e-mail: [fgis03700v@istruzione.it](mailto:fgis03700v@istruzione.it) – pec: [fgis03700v@pec.istruzione.it](mailto:fgis03700v@pec.istruzione.it) Web: [www.polotecnologico-sansevero.gov.it](http://www.polotecnologico-sansevero.gov.it)

Tel 0882 222860 Fax 0882 240971

C.F./P.IVA 03800890711 - Codice Meccanografico **FGIS03700V**

---

**MINACCE A CUI SONO SOTTOPOSTI I SUPPORTI DI MEMORIZZAZIONE**

Le principali minacce ai supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Il Dirigente Scolastico  
Prof. Vincenzo CAMPAGNA  
Firma autografa sostituita a mezzo stampa  
ai sensi dell'art. 3, c.2 del D. Lgs. n.39/93