



BIPLANO Società Cooperativa Sociale

**DOCUMENTO PROGRAMMATICO sulle MISURE di SICUREZZA
ADOTTATE per il TRATTAMENTO dei DATI PERSONALI**

In base al disciplinare tecnico in materia di misure minime di sicurezza
(Allegato B) del D. lgs. 30-06-03 n. 196

* * *

Il sottoscritto Giacomo Ribaudo, in qualità di Presidente del C.d.A. della Società Cooperativa Sociale Biplano, con sede in Via BATTAINA 901 24059 URGANO (BG), P.I. / C.F. 02658860164, REA BG – 312827, iscritta all'Albo delle Cooperative Sociali della Provincia di Bergamo sezione B n° 848 in data 08/07/2013. Per la sezione A: iscritta all'Albo Regionale delle Cooperative Sociali n° 246, decreto prefettizio n° 492 in data 22/07/1999, n° 333 sez. Coop. Produzione Lavoro, n° 114 sez. Sociale. Iscritta all'Albo nazionale delle Cooperative Sociali a mutualità permanente n° A113983 dal 22/07/1999 nella categoria Cooperative Sociali.

in considerazione

dell'obbligo di adottare gli accorgimenti per garantire le misure minime di sicurezza previste dagli articoli 33-36 del D. lgs. 30-06-2003 n. 196 al fine di proteggere gli archivi elettronici e cartacei contenenti i dati personali

REDIGE il seguente

DOCUMENTO PROGRAMMATICO

INDICE

1 ELENCO DEI TRATTAMENTI DEI DATI PERSONALI	3
1.1 Informazioni essenziali.....	3
1.2 Ulteriori elementi per descrivere gli strumenti.....	4
1.3 Postazioni informatiche/Strutture	4
2 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ.....	5
3 ANALISI DEI RISCHI CHE INCOMBONO SUI DATI.....	6
4 MISURE IN ESSERE E DA ADOTTARE	7
4.1 Scheda descrittiva delle misure da adottare.....	7
5 CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI	8
6 PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI	8
6.1 Informazioni essenziali.....	8
7 TRATTAMENTI AFFIDATI ALL'ESTERNO	9
8 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI	10
9 PROCEDURE PER LA SICUREZZA DEL TRATTAMENTO DEI DATI.....	10
9.1 Protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità.....	10
9.2 Gestione strumenti elettronici.....	11
9.2.1 Antivirus	11
9.2.2 Sistema operativo	11
9.2.3 Altri software	11
9.2.4 Firewall e sistemi di anti intrusione.....	12
9.2.5 Gestione supporti rimovibili contenenti dati sensibili	12
9.2.6 Gestione manutenzione strumenti elettronici.....	12
9.2.7 Sistema di identificazione e autenticazione	12
9.3 Trattamenti senza l'ausilio di strumenti elettronici	13
9.4 Criteri e modalità di ripristino della disponibilità dei dati.....	13
9.4.1 Backup dati	13
10 CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA	14
11 MODALITÀ AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA.....	14
12 ALLEGATI	15
• Regolamento di utilizzo degli strumenti elettronici e gestione dei documenti cartacei.....	15
• Nomina del Responsabile per il trattamento dei dati	18

- Istruzione e nomina Incaricato interno 19

1 ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

In base alla **regola 19.1** del disciplinare tecnico, il Titolare (Società Cooperativa Sociale BIPLANO) ha provveduto all'elencazione di tutti i trattamenti, effettuati direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

1.1 Informazioni essenziali

Codice	Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
	Finalità perseguita o attività svolta	Categorie di interessati	S	G			
01	Approvvigionamento di beni e/o servizi	Fornitori	S		Segreteria amministrativa Via Battaina 901 24059 URGANO BG		PC, rete LAN con accesso a Internet
							Archivi cartacei
02	Gestione del Personale Rapporto Soci Tirocinanti Inserimenti lavorativi	Personale Soci Tirocinanti Inserimenti	S	G	Segreteria amministrativa Via Battaina 901 24059 URGANO BG	COESI Servizi Via San Bernardino 59 24122 BERGAMO BG	PC, rete LAN con accesso a Internet
							Archivi cartacei
03	Fornitura di beni e servizi	Clienti Utenti	S	G	Segreteria amministrativa Via Battaina 901 24059 URGANO BG		PC, rete LAN con accesso a Internet
							Archivi cartacei
01 02 03	Approvvigionamento di beni e/o servizi Gestione del Personale Fornitura di beni e servizi	Tutti	S	G	Direzione Via Battaina 901 24059 URGANO BG		PC, rete LAN con accesso a Internet
							Archivi cartacei
03	Fornitura di servizi Agricoltura Sociale Comunità Riabilitativa Centro Diurno Residenzialità leggera	Clienti Utenti Tirocinanti Inserimenti	S	G	Responsabili di Area Via Battaina 901 24059 URGANO BG Via Daste e Spalenga 14 24020 GORLE BG		PC, rete LAN con accesso a Internet
							Archivi cartacei

1.2 Ulteriori elementi per descrivere gli strumenti

Codice	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi d'accesso
01	Archivio fornitori. Documento elettronico. Documenti cartacei Programma di gestione: Office	Segreteria amministrativa, Direzione Via Battaina 901 24059 URGNANO BG	Personal Computer SO Windows Microsoft
01	Banca dati fornitori. Programma di gestione: Office	Segreteria amministrativa Via Battaina 901 24059 URGNANO BG	Personal Computer SO Windows Microsoft
02	Archivio personale. Documento elettronico Programma di gestione: Office	Segreteria amministrativa, Direzione Via Battaina 901 24059 URGNANO BG	Personal Computer SO Windows Microsoft
02	Banca dati personale. Programma di gestione: Office	Segreteria amministrativa, Direzione Via Battaina 901 24059 URGNANO BG	Personal Computer SO Windows Microsoft
03	Archivio e documenti clienti/utenti. Documento elettronico Programma di gestione: Office	Segreteria amministrativa, Direzione Via Battaina 901 24059 URGNANO BG	Personal Computer SO Windows Microsoft
03	Archivio e documenti clienti/utenti. Documento elettronico Programma di gestione: Office	Responsabili di Area Via Battaina 901 24059 URGNANO BG Via Daste e Spalenga 14 24020 GORLE BG	Personal Computer SO Windows Microsoft

1.3 Postazioni informatiche/Strutture

Strutture e/o Servizi	
Segreteria Amministrativa	PC 5
Direzione	PC 1
Responsabili Aree Servizi	PC 5

Totale computer: 9 Personal Computer

2 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

In base alla regola 19.2 il Titolare (Società Cooperativa Sociale BIPLANO) ha descritto sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

Struttura	Codice trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Segreteria Amministrativa, Direzione	01, 02, 03	Acquisizione e caricamento dati relativi a fornitori, clienti/utenti e personale, consultazione per il normale svolgimento dell'attività lavorativa, comunicazione a terzi per la gestione dell'amministrazione e del personale, manutenzione tecnica dei programmi (aggiornamento, acquisto...), gestione tecnica operativa della base dati (salvataggio, ripristino...)
Responsabili Aree Servizi	03	Acquisizione e caricamento dati relativi a clienti/utenti, fornitori e personale, consultazione per il normale svolgimento dell'attività lavorativa, comunicazione a terzi per la gestione dell'erogazione dei servizi, gestione tecnica operativa della base dati (salvataggio, ripristino...)

3 ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

In base alla regola 19.3 la Cooperativa BIPLANO opera in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

Rischi	SI/NO	Descrizione dell'impatto sulla sicurezza (<i>gravità: alta, media, bassa</i>)
Comportamento degli operatori		
Sottrazione di credenziali di autenticazione	SI	Rischio furto dati. Gravità Bassa
Carenza di consapevolezza, disattenzione o incuria	SI	Rischio perdita dei dati. Gravità Bassa
Comportamenti sleali o fraudolenti	SI	Rischio furto dati. Gravità Bassa
Errore materiale	SI	Rischio perdita dati. Gravità Media
Eventi relativi agli strumenti		
Azione di virus informatici o di programmi suscettibili di recare danno	SI	Rischio danneggiamento o perdita dati. Gravità Media
Spamming o tecniche di sabotaggio	SI	Rischio danneggiamento, sottrazione o perdita dati. Gravità Bassa
Malfunzionamento, indisponibilità o degrado degli strumenti	SI	Rischio danneggiamento o perdita dati. Gravità Bassa
Accessi esterni non autorizzati	SI	Rischio danneggiamento o perdita dati. Gravità Bassa
Intercettazioni di informazioni in rete	SI	Rischio danneggiamento, sottrazione o perdita dati. Gravità Bassa
Eventi relativi al contesto		
Accessi non autorizzati a locali ad accesso ristretto	SI	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità Bassa
Sottrazione di strumenti contenenti dati	SI	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità Bassa
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti a incuria	SI	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità Bassa
Guasto ai sistemi complementari/ausiliari	SI	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità Bassa
Errori umani nella gestione della sicurezza fisica	SI	Rischio danneggiamento o perdita dati informatici e cartacei. Gravità Bassa

4 MISURE IN ESSERE E DA ADOTTARE

In base alla regola 19.4 il Titolare (Società Cooperativa Sociale BIPLANO) ha indicato quali misure ha già predisposte e quali adotterà per contrastare i rischi individuati.

Descrizione rischi	Misure	Trattamenti interessati	Misure già in essere	Misure da adottare	Struttura o persone addette all'adozione
Comportamento degli operatori	Redazione delle Procedure per la sicurezza. Assegnazione dell'incarico di Responsabile Privacy e di Incaricato/i	01, 02, 03	X		La Direzione redige le Procedure interne per la sicurezza e nomina il Responsabile per la Cooperativa e gli Incaricati al trattamento
	Sistemi di protezione accesso (user ID, password)		X		Il Responsabile e gli Incaricati al trattamento.
	Sistemi di salvataggio dati		X		Segreteria Amministrativa, Direzione e Responsabili.
	Formazione		X		Amministratori, Responsabile, Incaricati al trattamento
Eventi relativi agli strumenti	Utilizzo Firewall.	01, 02, 03	X		Segreteria Amministrativa, Direzione e Responsabili
	Utilizzo Antivirus		X		Segreteria Amministrativa, Direzione e Responsabili
	Revisione e aggiornamento PC e periferiche		X		Segreteria Amministrativa e Direzione
			X		Responsabili
Eventi relativi al contesto	Protezione fisica dei locali, delle attrezzature e dei dati	01, 02, 03	X		Direzione e Responsabili

4.1 Scheda descrittiva delle misure da adottare

Misura	Descrizione	Tempi attuazione

5 CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

In base alla regola 19.5 il Titolare (Società Cooperativa Sociale BIPLANO) ha indicato i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.

Data base e /o archivio dati	Strutture	Criteri minimi per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
Fornitori	Segreteria Amministrativa, Direzione	Backup giornaliero su HD esterno. Salvataggio giornaliero su server.	Semestrale
Personale	Segreteria Amministrativa, Direzione	Backup giornaliero su HD esterno. Salvataggio giornaliero su server.	Semestrale
Clienti/Utenti	Segreteria Amministrativa, Direzione	Backup giornaliero su HD esterno. Salvataggio giornaliero su server.	Semestrale
Clienti/Utenti	Resp. Aree Servizi	Backup giornaliero su HD esterno. Salvataggio giornaliero su server.	Semestrale

6 PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

In base alla regola 19.6 il Titolare (Società Cooperativa Sociale BIPLANO) ha stabilito quali interventi formativi ritiene opportuno pianificare in relazione a specifici gli obiettivi e le modalità dell'intervento formativo.

6.1 Informazioni essenziali

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti

7 TRATTAMENTI AFFIDATI ALL'ESTERNO

In base alla regola 19.7 il Titolare (Società Cooperativa Sociale BIPLANO) ha descritto sinteticamente le attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Consulenza del lavoro e Gestione del Personale (paghe e contributi)	Dati personali e sensibili del personale	COESI Servizi Via San Bernardino 59 24122 BERGAMO BG	La Cooperativa è partner di COESI che ha come <i>mission</i> quella della tutela e del supporto delle cooperative clienti. COESI si è impegnato e adotta tutte le misure necessarie alla protezione dei dati personali utilizzati, finalizzati all'erogazione di servizi alle proprie associate/clienti.

8 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI

Il Sig.

Nome	Giacomo	Cognome	Ribaudo
-------------	---------	----------------	---------

è stata nominata in data 02-05-2017 RESPONSABILE DEL TRATTAMENTO a tutti gli effetti legali, secondo i criteri, le modalità e le istruzioni di seguito specificate nel documento di nomina allegato in questo documento programmatico sulla sicurezza.

Si è valutato che il medesimo sia in possesso dei requisiti di esperienza, capacità ed affidabilità richiesti dal comma 2 dell'art. 29 del D.Lgs. 196/2003.

I signori:

NOME E COGNOME	AREA/SERVIZIO
Giacomo Ribaudo	Direzione
Cinzia Morosini	Segreteria Amministrativa
Luciano Maffioletti	Agricoltura Sociale
Luca Fornoni	CRM
Daniela Gladi	Centro Diurno
Cristina Chillè	Centro Diurno
Licia De Angelis	Residenzialità Leggera

Sono stati nominati INCARICATI DEL TRATTAMENTO

In questo ruolo e nei limiti delle mansioni a loro affidate, tali soggetti potranno eseguire le operazioni di trattamento riguardanti le sopraddette banche dati, attenendosi alle istruzioni impartite dal Titolare o dal Responsabile del trattamento. Nel singolo documento di nomina allegato, sono evidenziate le operazioni riguardanti il trattamento di dati personali di propria competenza e le banche dati a cui il singolo Incaricato può accedere.

9 PROCEDURE PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

9.1 Protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità

L'accesso fisico alle stanze contenenti documenti trattanti dati personali è permesso solo agli incaricati del trattamento.

Gli armadi in cui sono detenuti documenti cartacei inerenti dati personali devono essere dotati di serratura a chiave.

Il Responsabile del trattamento si occupa della gestione delle chiavi in oggetto.

9.2 Gestione strumenti elettronici

9.2.1 Antivirus

La Cooperativa si è dotata del seguente software:

Nome prodotto antivirus in dotazione	Karspersky
Descrizione prodotto	L'antivirus in oggetto controlla in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali cd-rom e chiavette
Modalità di aggiornamento	L'aggiornamento del prodotto antivirus installato è continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.
Incaricato aggiornamento	Responsabile e Incaricati

9.2.2 Sistema operativo

La Cooperativa si è dotata dei seguenti sistemi operativi:

Nome prodotto in dotazione	Windows XP e Windows 10
Descrizione prodotto	Sistema operativo
Modalità di aggiornamento	L'aggiornamento del prodotto installato è continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.
Incaricato aggiornamento	Direzione e Responsabili del Servizio-Amministrazione

9.2.3 Altri software

Nome prodotto in dotazione	Microsoft Office 2013
Descrizione prodotto	Applicazioni per la realizzazione di testi, fogli di calcolo ecc.
Modalità di aggiornamento	L'aggiornamento del prodotto installato è continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.
Incaricato aggiornamento	Direzione e Responsabili del Servizio-Amministrazione
Nome prodotto in dotazione	Gescop
Descrizione prodotto	Gestione cartellini presenze
Modalità di aggiornamento	L'aggiornamento del prodotto è garantito dalla possibilità di richieste di assistenza alla ditta produttrice, sia on-site che da remoto.
Frequenza aggiornamento	Stabilita dal produttore
Incaricato aggiornamento	Responsabili del Servizio-Amministrazione

Nome prodotto in dotazione	Mago
Descrizione prodotto	Gestione contabilità generale e magazzino, gestione clienti, fatturazione
Modalità di aggiornamento	L'aggiornamento del prodotto installato è garantito dalla possibilità di richieste di assistenza alla ditta produttrice, sia on-site che da remoto.
Frequenza aggiornamento	Stabilita dal produttore
Incaricato aggiornamento	Responsabili del Servizio-Amministrazione

9.2.4 Firewall e sistemi di anti intrusione

La Cooperativa si è dotata del seguente sistema firewall

Nome prodotto	Funzione di Windows Firewall Hardware sulla rete LAN
Incaricato alla gestione e all'aggiornamento	Direzione tramite incaricati assistenza software

9.2.5 Gestione supporti rimovibili contenenti dati sensibili

Nel regolamento operativo allegato sono state fornite istruzioni organizzative e tecniche ad hoc per la custodia e l'uso di supporti rimovibili contenenti dati sensibili e giudiziari (floppy disk, chiavette hard disk, cd riscrivibili, ecc.).

9.2.6 Gestione manutenzione strumenti elettronici

La manutenzione degli strumenti elettronici viene affidata alla ditta:

Ragione sociale	PC Assistance
Indirizzo	Via Garibaldi 35 24068 Seriate BG
Partita IVA	13314630156

9.2.7 Sistema di identificazione e autenticazione

La Cooperativa ha attivato un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali.

È stato attribuito un codice identificativo (username, user ID) strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico della Cooperativa.

I codici identificativi sono frequentemente aggiornati, inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati.

Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) sia a livello di sistema operativo sia a livello di singola applicazione.

Il Responsabile del trattamento è Incaricato della gestione delle password.

Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso.

Si sollecita l'Incaricato che riceve una password a modificarla al primo utilizzo.

L'Incaricato deve segnalare al Responsabile del trattamento o al custode nominato la sua password in uso.

Viene segnalato ad ogni Incaricato la necessità di cambiare la password almeno ogni 6 mesi.

Nell'ipotesi di trattamento di dati sensibili viene segnalato ad ogni Incaricato la necessità di cambiare la password almeno ogni 3 mesi.

È prevista una scadenza nella validità di ogni password utilizzata in Cooperativa.

Sono vietate in Cooperativa credenziali di autenticazione (username e password) condivise fra più persone.

Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate.

Le credenziali di autenticazione vengono immediatamente revocate in caso di provvedimenti disciplinari o quando si presentano situazioni che possono compromettere la sicurezza.

Sono state consegnate istruzioni scritte agli incaricati in merito alle modalità di gestione e di custodia delle password.

In caso di prolungata assenza dell'Incaricato, il Responsabile del trattamento è autorizzato ad rivelare la password in uso per assicurare la disponibilità dei dati e degli strumenti elettronici.

La visualizzazione della password sullo schermo dei personal computer è impedita da tutti i software in uso.

Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili e sui palmari che possono gestire e contenere dati personali.

9.3 Trattamenti senza l'ausilio di strumenti elettronici

Nella sezione "gestione documenti cartacei" del Regolamento di utilizzo degli strumenti elettronici allegato al presente documento, sono impartite agli incaricati istruzioni scritte, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli uffici, nei luoghi contenenti gli archivi contenenti dati sensibili o giudiziari sono identificate e registrate.

Il Responsabile del trattamento è incaricato della gestione delle autorizzazioni nei luoghi contenenti archivi di dati sensibili.

9.4 Criteri e modalità di ripristino della disponibilità dei dati

9.4.1 Backup dati

Al fine di garantire non solo la integrità, ma anche la pronta disponibilità dei dati, la Cooperativa si è dotata di strumenti e procedure di backup.

Si è valutata il sistema e la capienza dello strumento scelto più che sufficiente per la mole di dati attualmente gestita dalla Cooperativa stessa.

Tutti i dati personali gestiti con strumenti elettronici nella Cooperativa vengono inclusi nella procedura di backup.

La frequenza con cui vengono effettuate le copie di sicurezza è mensile. I supporti di backup vengono titolati e la loro custodia etichettata. Ogni volta viene effettuata dal Responsabile del trattamento una verifica della leggibilità ed integrità del supporto di backup.

Le copie di backup non sono conservate nello stesso luogo fisico ove si trovano gli strumenti elettronici con cui si gestiscono i dati personali ma vengono depositate dal Responsabile del trattamento

Luogo custodia	Abitazione del Responsabile
----------------	-----------------------------

Il tempo massimo per la conservazione delle copie di backup è stato stabilito:

Tempo massimo conservazione	6 mesi
-----------------------------	--------

Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento negativo, comunque ampiamente sotto il limite dei sette giorni previsti dal punto 23 dell'allegato B del D.Lgs. 196/2003 in ipotesi di trattamento di dati sensibili.

10 CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Il Responsabile mantiene aggiornate le misure di sicurezza al fine di adottare gli strumenti più idonei per la tutela dei dati trattati.

Egli verifica inoltre con frequenza almeno mensile l'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento
- procedure di archiviazione e custodia dati trattati
- efficacia e utilizzo misure di sicurezza strumenti elettronici
- integrità dei dati e delle loro copie di backup
- distruzione dei supporti magnetici non più riutilizzabili
- livello di informazione degli interessati

11 MODALITÀ AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

Il presente documento redatto in data odierna, viene firmato in calce dal Presidente della Cooperativa in qualità di Titolare e verrà aggiornato ogni volta che vi siano cambiamenti significativi nella Cooperativa impattanti sulle misure minime di sicurezza.

Il Responsabile è il soggetto preposto all'aggiornamento e alla custodia del documento programmatico per la sicurezza.

Nel caso di cambiamenti organizzativi, apertura di nuovi servizi o cambio di personale, il Titolare del trattamento (od il Responsabile per la sicurezza se nominato) dovrà procedere alla completa revisione del documento in oggetto.

L'originale del presente documento è custodito presso la sede della Cooperativa, per essere esibito in caso di controllo. Una copia verrà consegnata ai responsabili di determinati trattamenti di dati appositamente nominati.

12 ALLEGATI

- **Regolamento di utilizzo degli strumenti elettronici e gestione dei documenti cartacei**

Premessa

I dipendenti, i collaboratori e i soci devono ispirarsi ad un principio generale di diligenza e correttezza nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo della Cooperativa. Ogni utilizzo del sistema informativo della Cooperativa diverso da finalità strettamente professionali è espressamente vietato.

Di seguito vengono esposte regole minime comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine della Cooperativa stessa.

La Cooperativa s'impegna a formare gli incaricati in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.

Il regolamento deve essere portato a conoscenza e distribuito a tutti i componenti della Cooperativa.

- Art. 1 -

FINALITA' DEL TRATTAMENTO DEI DATI "SENSIBILI"

La Cooperativa per l'esclusivo svolgimento delle proprie funzioni istituzionali effettua il trattamento di dati "sensibili" nell'ambito della erogazione di servizi di educazione, assistenza e cura, senza scopo di lucro, correlate ai servizi rivolti agli utenti (ospitati e non).

La Cooperativa effettua anche il trattamento di dati "sensibili" riguardanti il personale dipendente e non dipendente operante presso i Servizi al fine della regolare gestione del rapporto di lavoro dipendente o in convenzione o di volontariato.

- Art. 2 -

IDENTIFICAZIONE DATI "SENSIBILI" TRATTATI

Con riferimento alle finalità di interesse pubblico di cui all'art. 1 del presente regolamento ed ai sensi delle disposizioni della vigente normativa identifica i dati "sensibili", indicati nel capitolo 1 del presente documento, di cui è effettuato il trattamento presso l'ente.

- Art. 3 -

DATI TRATTATI

I dati trattati sono quelli essenziali allo svolgimento delle attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

- Art. 4-

OPERAZIONI PERTINENTI ED ESEGUIBILI

Le operazioni strettamente pertinenti nel trattamento dei dati "sensibili", previste dalla legge, sono quelle indispensabili all'erogazione delle prestazioni assistenziali e riabilitative agli utenti ed alla gestione dei rapporti di lavoro o in convenzione o di volontariato.

- Art. 5 –

INCARICATI DEL TRATTAMENTO

L'accesso e l'utilizzo dei dati "sensibili" è consentito ai soli incaricati del trattamento, preposti caso per caso alle specifiche fasi delle attività istituzionali dell'ente secondo il principio della pertinenza dei dati di volta in volta trattati.

Utilizzo dell'elaboratore e/o della rete interna

L'accesso all'elaboratore della propria postazione di lavoro, sia esso collegato in rete o "stand alone", è protetto da un sistema di autenticazione.

La Cooperativa ha attivato un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali.

È stato attribuito un codice identificativo (username, user ID) strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico della Cooperativa. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza. Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) sia a livello di sistema operativo sia a livello di singola applicazione. Il Responsabile del trattamento è Incaricato della gestione delle password.

Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso. Si sollecita l'Incaricato che riceve una password a modificarla al primo utilizzo. L'Incaricato deve segnalare al Responsabile del trattamento o al custode nominato la sua password in uso. Viene segnalato ad ogni Incaricato la necessità di cambiare la password almeno ogni 6 mesi.

È vietato installare qualsiasi software anche demo, senza autorizzazione.

Su ogni elaboratore della Cooperativa è stato installato un software antivirus ed un software ad-ware per prevenire eventuali danneggiamenti all'hardware o al software causati dalla presenza o dall'azione di programmi virus informatici. È importante utilizzare questi software antivirus per controllare qualsiasi file di provenienza esterna alla Cooperativa. È cura di ciascun operatore provvedere all'aggiornamento dei software, con cadenza minima settimanale, dell'antivirus installato.

Si ricorda che nonostante la presenza del software antivirus è possibile che riescano ugualmente ad installarsi nei computer virus informatici non identificati o riconoscibili. Pertanto in caso si evidenzino anomalie di funzionamento del computer è importante darne rapida segnalazione al Responsabile del trattamento.

L'elaboratore, le unità di rete e le aree di condivisione contengono informazioni strettamente professionali e non possono essere utilizzate per scopi diversi. Non bisogna dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (ad esempio i corridoi degli uffici).

Gestione supporti rimovibili contenenti dati sensibili

Senza specifica autorizzazione è fatto divieto di usare supporti rimovibili contenenti dati sensibili e giudiziari (floppy disk, chiavette hard disk, cd riscrivibili, ecc.).

Utilizzo servizi vari su internet

I servizi on line devono essere esclusivamente finalizzati al reperimento di informazioni utili alla Cooperativa.

Ogni altra utilizzazione dell'accesso su internet, non finalizzata al reperimento di informazioni utili alla Cooperativa, non pertinente all'attività lavorativa o di tipo personale non è consentita. Al fine di non compromettere la sicurezza della Cooperativa e di prevenire conseguenze legali o di altro genere a carico della stessa, gli utenti dovranno adottare i seguenti comportamenti:

- evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat, di bacheche elettroniche e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività professionale;

Utilizzo del servizio di posta elettronica

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Cooperativa ed in stretta connessione con l'effettiva attività e mansioni del soggetto dipendente o collaboratore che utilizza tale funzionalità.

Non è possibile utilizzare tale servizio per finalità in contrasto con quelle della Cooperativa, o non pertinenti all'attività lavorativa o personali.

Al fine di non compromettere la sicurezza della Cooperativa e di prevenire conseguenze legali a carico della stessa bisogna adottare le seguenti norme comportamentali:

- se nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono mail da destinatari sconosciuti contenenti file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi) evitare di aprire tali mail e tali file e procedere alla loro immediata eliminazione. Il comportamento sopradescritto va seguito anche se si ricevono file non concordati da destinatari conosciuti;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione;

Gestione dei documenti cartacei

La documentazione cartacea contenente dati personali o sensibili deve essere protetta in appositi armadi dotati di chiavi. Le chiavi devono essere conservate a cura del Responsabile dell'ufficio.

Ogni volta che un soggetto autorizzato preleva documenti contenenti dati sensibili da tali archivi è tenuto a lasciarne traccia mediante apposita segnalazione riportante il proprio nome, data e ora del prelevamento in un apposito registro.

Tutti i documenti contenenti dati personali o aziendali che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

È vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici, come per esempio corridoi o sale riunioni.

• **Nomina del Responsabile per il trattamento dei dati**

Egregio Sig.

Nome	Giacomo	Cognome	Ribaudo
------	---------	---------	---------

Ai sensi dell'art. 29 del decreto legislativo 196/2003 ed in base alle intese intercorse, in considerazione delle funzioni da Lei espletate nella Cooperativa, Le comunichiamo la nomina a Responsabile del Trattamento delle banche dati presenti in Cooperativa e di quelle che in futuro Le verranno affidate. Nel suo incarico dovrà attenersi alle istruzioni impartite e contenute nel DPS, ed in particolare:

1. catalogare analiticamente le banche dati con tutti gli elementi necessari, anche ai fini dell'eventuale notifica al Garante
2. individuare gli incaricati del trattamento e successivamente diramare le istruzioni scritte necessarie per un corretto, lecito, sicuro trattamento, in riferimento anche a quanto contenuto e prescritto nel DPS
3. attuare gli obblighi di informazione e acquisizione del consenso, quando richiesto, nei confronti degli interessati
4. ove necessario, predisporre la notificazione iniziale e le eventuali successive variazioni verificando l'esattezza e la completezza dei dati contenuti, predisporre la richiesta di autorizzazione preventiva al trattamento di dati sensibili da inviare al Garante
5. applicare le disposizioni contenute nelle autorizzazioni generali del Garante relative al trattamento dei dati sensibili e giudiziari
6. garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo n.196/2003, in ordine all'accesso ai dati e a tutti i diritti di aggiornamento, rettificazione, cancellazione e di opposizione
7. collaborare per l'attuazione delle prescrizioni del Garante
8. predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni dell'art. 31 del decreto legislativo n. 196/2003, nonché adeguare il sistema alle norme regolamentari in materia di sicurezza, curandone l'applicazione da parte degli incaricati

Nell'espletamento delle sue funzioni dovrà applicare le misure di sicurezza disposte dalla Cooperativa e, specificatamente, nella gestione delle parole chiave dovrà:

9. ricevere dai singoli incaricati del trattamento comunicazione riservata della sostituzione di password effettuata
10. custodire le stesse parole chiave con modalità (fisiche ed organizzative) atte a garantire la segretezza delle stesse parole chiave e la loro integrità (vedi D.P.S.)
11. intervenire sul profilo autorizzativo del singolo Incaricato per permettere alla Cooperativa, Titolare del trattamento, di accedere ai dati trattati da ogni Incaricato con le modalità fissate dalla Cooperativa stessa, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività in caso di prolungata assenza od impedimento dell'Incaricato che renda indispensabile ed indifferibile l'intervento
12. informare tempestivamente l'Incaricato dell'intervento di accesso realizzato

Data 02-05-2017 il Presidente Giacomo Ribaudo_____ il Responsabile Giacomo Ribaudo_____

- **Istruzione e nomina Incaricato interno**

Egregio Sig.

NOME E COGNOME	AREA/SERVIZIO	FIRMA	DATA
Giacomo Ribaudò	Direzione		02-05-2017
Cinzia Morosini	Segreteria Amministrativa		02-05-2017
Luciano Maffioletti	Agricoltura Sociale		02-05-2017
Luca Fornoni	CRM		02-05-2017
Daniela Gladi	Centro Diurno		02-05-2017
Cristina Chillè	Centro Diurno		02-05-2017
Licia De Angelis	Residenzialità Leggera		02-05-2017

Il decreto legislativo 30 giugno 2003 n. 196 sulla tutela della riservatezza nel trattamento di dati personali ha introdotto rilevanti obblighi a carico della Cooperativa, obblighi la cui inosservanza è sanzionata penalmente ed espone a responsabilità civili. Questo decreto ha la finalità di garantire che il trattamento di dati personali si svolga nel pieno rispetto dei diritti dell'interessato, sia esso persona fisica che società, ente od associazione. La legge prescrive (art. 30) che vengano impartite da parte del o del Responsabile specifiche istruzioni agli "incaricati interno del trattamento" e, cioè, a coloro che, nell'ambito dell'organizzazione stessa ed in relazione alle mansioni affidate, trattano dati personali sia mediante sistemi informatici che mediante documenti cartacei. Pertanto, nell'ambito delle mansioni a lei assegnate, viene designato "Incaricato del trattamento". Oltre al regolamento interno che è tenuto ad osservare le vengono impartite le seguenti istruzioni atte a garantire un trattamento lecito, corretto e sicuro dei dati.

Istruzioni specifiche sul trattamento dei dati

Le rammentiamo quanto disposto dall'art. 11 del D.Lgs. 196/2003 ex art. 9 legge 675/96 I dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi
- esatti e se necessario aggiornati
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati

Inoltre si richiede la Sua particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi, nonché procedure per il salvataggio dei dati
- modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali

Modalità operative da seguire per il trattamento dei dati

Al fine della corretta gestione dei dati in trattamento la invitiamo pertanto ad attenersi alle seguenti indicazioni:

- richiedere e utilizzare soltanto i dati necessari alla normale attività lavorativa
- custodire i dati oggetto del trattamento in luoghi non accessibili a non autorizzati
- non lasciare incustodito il proprio posto lavoro prima di aver provveduto alla messa in sicurezza dei dati
- non lasciare incustoditi e accessibili a terzi gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni di consultazione
- custodire e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici
- accertarsi che i terzi siano a conoscenza e abbiano autorizzato l'uso dei dati richiesti
- accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita
- non fornire telefonicamente o a mezzo fax dati senza specifica autorizzazione e/o identificazione del richiedente

Accesso a banche dati aziendali

Le banche dati cui è autorizzato ad accedere per effettuare i trattamenti (sia informatici che cartacei), sempre strettamente pertinenti alle mansioni svolte e per le finalità previste dalla Cooperativa, rispettando i principi fondamentali sanciti dall'art. 11 del decreto legislativo n.196/2003, sono le seguenti: archivio utenti, archivio fornitori. L'Incaricato per la Segreteria amministrativa potrà accedere inoltre all'archivio dipendenti.

Creazione nuove banche dati. Gestione programmi

Senza preventiva autorizzazione del Titolare o del Responsabile ove nominato non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste.

Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dalla Cooperativa e, pertanto, in conformità alle informazioni che la stessa ha comunicato agli interessati. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso elaborati dalla Cooperativa. L'Incaricato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

Comunicazione e diffusione dei dati

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, è autorizzata la comunicazione dei dati stessi esclusivamente ai soggetti esterni che la Cooperativa stessa indica. Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dalla Cooperativa.

Misure di sicurezza

Ogni Incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dalla Cooperativa, nonché quelle che in futuro verranno comunicate.

Sistemi informatici

Per ogni Incaricato viene creata una "credenziale di autenticazione" che consente l'accesso in rete ai dati, attraverso una procedura di autenticazione (login). A tal fine, ad ogni Incaricato è stata assegnata in via riservata una credenziale per l'autenticazione che consiste in un codice identificativo (user id) ed una parola chiave riservata (password). Tale parola chiave non va comunicata ad altri incaricati; le variazioni disposte autonomamente dallo stesso Incaricato con periodicità semestrale (trimestrale in caso di trattamento di dati sensibili o giudiziari) devono essere comunicate, sempre in modo riservato, al custode delle credenziali. La postazione informatica non va lasciata incustodita lasciando accessibili i dati; tutti i supporti magnetici utilizzati vanno riposti negli archivi; i supporti non più utilizzati possono essere eliminati solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili. Si ricorda che la Cooperativa, Titolare del trattamento, nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dall'Incaricato ed agli strumenti informatici in dotazione allo stesso sia per le esigenze produttive associative sia per la sicurezza ed operatività dello stesso sistema

informatico (ad esempio nei casi di prolungata assenza od impedimento dell'Incaricato), potrà accedere mediante intervento del custode delle credenziali nominato dalla Cooperativa stessa. L'Incaricato non può installare ed utilizzare programmi per elaboratore non autorizzati dalla Cooperativa e né privi di licenza che legittimino l'uso. Gli strumenti informatici e telematici messi a disposizione costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate.

Trattamenti cartacei

In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, potrà accedere agli archivi relativi alle banche dati di tipo cartaceo ubicate presso le sedi della Cooperativa.

L'Incaricato nel trattare documenti contenenti dati sensibili o giudiziari è tenuto a custodirli fino alla restituzione in modo da evitare l'accesso agli stessi dati a persone prive di autorizzazione. L'Incaricato deve, inoltre, custodire gli archivi contenenti documenti con dati sensibili e giudiziari, ed evitare che personale non autorizzato vi acceda. L'accesso fuori dall'orario di lavoro impone la registrazione e identificazione delle persone ammesse ai locali. I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dalla Cooperativa.

● In merito alle **Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema** (27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009), il Titolare (Cooperativa Biplano) non ha provveduto a nominare gli Amministratori di Sistema, in quanto la rete dei PC desktop e portatili non si configura come "sistema", non vengono registrati accessi logici, i dati non vengono catalogati, trattati o utilizzati per altro scopo se non l'erogazione degli stessi servizi o per la gestione dei normali rapporti di lavoro.

Data 02-05-2017 il Responsabile Giacomo Ribaudò _____ il Presidente Giacomo Ribaudò _____