

 PROGETTI E SOLUZIONI	POLICY			PL-5.2-06	
	USER POLICY			Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato	Pagina : 1 di 17

REDATTO	APPROVATO
Responsabile SGI (RSGI)	General Manager (DIR)
R. Ragone	S. Bonasegale

TABELLA DELLE REVISIONI DEL DOCUMENTO

REV.	DATA	DESCRIZIONE MODIFICHE
0	20.04.2023	Supera la PR_421-02_Ed_28_=SC_RSI_I_User Policy
1	26/08/2024	Definite modalità di cancellazione sicura dispositivi usati. Cambio logo e denominazione dell'azienda.

SISTEMI DI GESTIONE APPLICABILI	<input type="checkbox"/> ISO 9001	<input type="checkbox"/> ISO 14001	<input type="checkbox"/> ISO 37001	<input checked="" type="checkbox"/> ISO 22301
	<input checked="" type="checkbox"/> ISO/IEC 27001 con estensioni ISO/IEC 27017 e ISO/IEC 27018			
MODELLI NORMATIVI APPLICABILI	<input checked="" type="checkbox"/> GDPR (Reg.UE 2016/679)			<input checked="" type="checkbox"/> d.lgs.231/01

INDICE

1 GENERALITÀ	3
1.1 Finalità della policy	3
1.2 Destinatari della policy	3
1.3 campo di applicazione	3
2 RESPONSABILITÀ E NORMATIVE DI RIFERIMENTO	3
2.1 Rispetto procedure di Sicurezza	4
3 NORME COMPORTAMENTALI	4
3.1 Utilizzo asset e comportamento professionale	4
3.2 Clear desk policy	4
3.3 Utilizzo dei sistemi di riproduzione	4
3.4 Clear screen policy	5
3.5 Chiavi fisiche e codici di sicurezza antintrusione	5
4 PROTEZIONE DI INFORMAZIONI E DATI PERSONALI	5
4.1 Clausole contrattuali sulla riservatezza delle informazioni	6
5 MODALITÀ DI ACCESSO DEI DIPENDENTI E DEGLI OSPITI ALLE STRUTTURE	6
6 SICUREZZA DEI SISTEMI INFORMATIVI	7
6.1 Gestione della credenziali di accesso	7
6.2 Regole di utilizzo delle Credenziali	7
6.3 Regole di utilizzo delle Password	7
6.4 Token OTP su Google Authenticator (One Time Password)	7
6.5 Internet	8
6.6 Regole di upload su FTP e monitoraggio	9
6.7 Fonti di Informazioni su Internet	9
6.8 Intranet	9
6.9 Posta elettronica	9
6.10 Uso personale	11
6.11 Accesso Remoto	12
6.12 Telelavoro e smart working	12
7 UTILIZZO DELLE POSTAZIONI DI LAVORO	12

 PROGETTI E SOLUZIONI®	POLICY		PL-5.2-06	
	USER POLICY			Rev. 1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
			Pagina :	2 di 17

7.1	Hardware	12
7.2	Smartphone	13
7.3	Strumenti di supporto.....	14
7.4	Dismissione e riuso dei dispositivi	14
7.5	Software.....	14
7.6	Antivirus	15
8	CONTROLLO E MONITORAGGIO DELLE RISORSE.....	16
9	VIOLAZIONE DELLA POLICY.....	17

 PROGETTI E SOLUZIONI	POLICY	PL-5.2-06		
	USER POLICY		Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
			Pagina :	3 di 17

1 GENERALITÀ

1.1 FINALITÀ DELLA POLICY

Lo scopo del presente documento è disciplinare le condizioni ed i limiti entro cui gli utenti possono legittimamente usare le informazioni aziendali, le postazioni di lavoro, i servizi Internet/Intranet ed ogni altro strumento o dispositivo informatico e telematico messo a disposizione dall'azienda, evitando di esporre se stessi e/o Progetti e Soluzioni a sanzioni pecuniarie e/o penali o in generale ridurre il livello di sicurezza dell'organizzazione.

1.2 DESTINATARI DELLA POLICY

Questa policy è valida per tutto il personale e per ogni altra persona autorizzata, anche in via temporanea, ad usare le attrezzature e i sistemi di Progetti e Soluzioni SpA. Queste persone verranno indicate come "Utenti". In caso l'Utente faccia parte di una società la User Policy si estende a tutti i soci e il firmatario accetta in nome e per conto di tutti i soci.

Il presente documento dovrà essere letto e sottoscritto dai destinatari.

L'accesso alla postazione di lavoro, informazioni, sistemi/servizi, da parte degli utenti, non potrà avvenire senza aver preventivamente recepito le prescrizioni e le indicazioni ivi contenute.

1.3 CAMPO DI APPLICAZIONE

Il regolamento deve essere recepito ed applicato dagli utenti che utilizzano, a qualsiasi titolo, le risorse informative aziendali. Per risorse si intendono:

- Postazioni di lavoro;
- Hardware e periferiche (stampanti, memorie di massa, altri supporti etc.);
- Dispositivi mobile (Smartphone, tablet, etc)
- Software;
- Informazioni e documentazione;
- Servizi informativi (posta, directory aziendale, portali interni, server, Internet, etc...);
- Infrastrutture fisiche
- Rete
- Risorse umane

Le norme indicate sono parte integrante del Sistema di Gestione Integrato, promosso e progettato dalla Direzione Aziendale.

2 RESPONSABILITÀ E NORMATIVE DI RIFERIMENTO

Di seguito sono illustrati gli oneri e le regole comportamentali, divise per ambiti (organizzativi, tecnologici, di servizio), che l'Utente è tenuto a rispettare durante l'espletamento delle proprie mansioni aziendali. In nessun caso, volontariamente o meno, l'utilizzo da parte degli utenti del Sistema Informativo Aziendale potrà essere in contrasto con quanto stabilito dalle normative di riferimento:

- Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica, Legge 48/2008 (Legge sui Reati Informatici)
- Regolamento UE 679/2016 (GDPR) e D.Lgs. 101/2018 sulla privacy
- Legge 300/1970 (tutela della libertà e dignità dei lavoratori)
- Legge n. 633/1941 (Tutela del diritto d'autore)
- Art 2049 c.c. e Art 40 c.p.: il datore di lavoro è responsabile delle azioni del dipendente; "reati omissionis"
- D.Lgs. 231/2001 - Responsabilità amministrativa da reato (a tale proposito, è necessario che il dipendente legga e sottoscriva anche il Codice Etico di Progetti e Soluzioni)

L'Utente, *autorizzato* ad accedere alle risorse di Progetti e Soluzioni, deve essere consapevole delle conseguenze derivanti da azioni e comportamenti illeciti o non conformi al presente regolamento.

In particolare, in base alla legge n. 547/1993 (Legge sui crimini informatici) le conseguenze penali si possono tradurre in pene, proporzionali al reato commesso, fino a 8 anni di reclusione.

 PROGETTI E SOLUZIONI	POLICY			PL-5.2-06	
	USER POLICY			Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato	Pagina : 4 di 17

2.1 RISPETTO PROCEDURE DI SICUREZZA

L'Utente accetta e si impegna a rispettare le procedure e le politiche di sicurezza fornite dall'organizzazione, contribuendo al mantenimento della sicurezza delle informazioni.

3 NORME COMPORTAMENTALI

3.1 UTILIZZO ASSET E COMPORTAMENTO PROFESSIONALE

L'utilizzo degli strumenti e delle risorse aziendali deve essere strettamente vincolato all'esercizio delle attività lavorative.

È proibito:

- L'impiego delle risorse aziendali per **scopi personali o di terzi**; in particolare
- Installare, sulle postazioni di lavoro in dotazione, software non licenziato e, comunque, **non esplicitamente autorizzato** dalle funzioni competenti;
- Impiegare le risorse per finalità diverse da quelle per le quali sono state progettate o utilizzate i sistemi informativi per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, all'organizzazione;
- Recare volontariamente danni alle risorse aziendali, agli strumenti di supporto, ai locali ed in generale ai dispositivi informatici utilizzati dall'organizzazione.

Ogni strumento o risorsa, concessa ai fini esclusivamente lavorativi, deve essere **correttamente custodito e mantenuto** in buono stato dall'Utente che deve contribuire, in rapporto alle proprie responsabilità, alla protezione dell'intero patrimonio di Gruppo Progetti e Soluzioni.

È onere dell'Utente richiedere gli interventi di manutenzione opportuni, segnalando tale necessità alla struttura competente.

Tutte le dotazioni, fornite all'Utente, risorse informatiche e tecnologiche, informazioni, documentazione, sono di proprietà di Progetti e Soluzioni; l'Utente è consapevole ed accetta di restituire la totalità delle risorse utilizzate nel momento in cui cessa il rapporto con Progetti e Soluzioni.

Gli utenti **non devono, inoltre, memorizzare "informazioni personali"** (ai sensi del Regolamento UE 679/2016 e del D.Lgs. 101/2018 sulla privacy), sui sistemi informativi di proprietà dell'organizzazione, al fine di ridurre al minimo l'esposizione dell'organizzazione ai vincoli normativi sul trattamento dei dati personali.

È responsabilità degli utenti segnalare immediatamente al Responsabile per la Sicurezza delle Informazioni o al Responsabile del Sistema Informativo Aziendale ogni attività sospetta o non conforme alle suddette politiche.

3.2 CLEAR DESK POLICY

Durante l'espletamento della propria attività lavorativa, l'Utente deve prestare attenzione a **non divulgare accidentalmente informazioni aziendali** a personale non autorizzato, eventualmente presente nelle immediate vicinanze.

Nel caso di assenza prolungata, e comunque al termine della normale attività lavorativa giornaliera, l'Utente deve **rimuovere dalla propria area di lavoro le informazioni e i documenti**, di cui dispone, riponendole in luoghi idonei (armadi o cassettiere con serratura, casseforti, etc). I documenti che contengono informazioni ad accesso limitato o riservate non devono essere, in nessun caso, lasciati incustoditi sulle scrivanie.

3.3 UTILIZZO DEI SISTEMI DI RIPRODUZIONE

Limitare la produzione di stampe ai casi di effettiva necessità, specialmente se di documenti ad accesso limitato o riservati o contenenti informazioni riservate. L'Utente deve applicare le medesime disposizioni e politiche di sicurezza anche alle copie dei documenti originali.

In caso di stampe contenenti **dati riservati o dati personali di qualunque tipo**, le stesse devono essere conservate con cura da parte di chi effettua il trattamento del dato fino a quando è necessario che il dato sia conservato su carta. Tali stampe **devono essere distrutte** non appena questa necessità cessa, tramite gli appositi distruggi-documenti in dotazione agli uffici, secondo quanto previsto dalla PO-5.2-05 Policy di classificazione delle informazioni.

Durante la stampa, fotocopia o trasmissione via email di informazioni non pubbliche, da/a postazioni remote, l'Utente deve presidiare ed assistere all'intero processo, in modo da impedire la volontaria o accidentale

 PROGETTI E SOLUZIONI	POLICY			PL-5.2-06	
	USER POLICY			Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato	Pagina : 5 di 17

perdita di riservatezza sulle informazioni cartacee stampate. A tal riguardo è dovere dell'Utente **prelevare immediatamente i fogli riprodotti da stampanti e fotocopiatrici**.

Nel caso specifico di informazioni classificate come confidenziali o esclusive queste non devono essere stampate su stampanti di rete/centralizzata, a meno che non ci sia una persona autorizzata che controlli il processo di stampa e che provveda quindi a garantire la confidenzialità delle informazioni stampate.

3.4 CLEAR SCREEN POLICY

Il personal computer non deve essere lasciato incustodito durante una sessione di lavoro. Anche in caso di breve assenza, il **computer deve essere bloccato** tramite le funzionalità offerte dal sistema operativo (es. "blocca computer" tramite pressione contemporanea dei tasti **Ctrl+Alt+Canc**).

È consigliabile, inoltre, ogni qualvolta ci si allontana dal posto di lavoro, **sconnettersi anche dagli applicativi in uso**.

È vietato l'uso di **screen saver** diversi da quelli standard forniti dal sistema operativo.

Al termine della giornata lavorativa, l'Utente è tenuto a spegnere la postazione o quantomeno a chiudere le sessioni di lavoro (**logoff**).

3.5 CHIAVI FISICHE E CODICI DI SICUREZZA ANTINTRUSIONE

I dipendenti a cui è stata assegnata una chiave fisica di accesso ai locali e/o agli archivi fisici sono tenuti a custodirle con la massima diligenza, a non lasciarle incustodite né in ufficio né all'esterno e a non farne duplicati. La chiave andrà restituita alla fine del rapporto di lavoro o in caso di cambio sede e/o di mansione lavorativa, su richiesta della Direzione aziendale.

I dipendenti che sono stati messi a conoscenza del codice di disinserimento del sistema di allarme della propria sede di appartenenza sono tenuti a non comunicarlo a nessuno. Nel caso in cui il dipendente abbia necessità di accedere agli uffici al di fuori dell'orario lavorativo è tenuto a comunicare preventivamente l'accesso al responsabile incaricato dalla Direzione, al fine di evitare falsi allarmi da parte dell'istituto di vigilanza.

4 PROTEZIONE DI INFORMAZIONI E DATI PERSONALI

Nell'ambito del rapporto di lavoro con Progetti e Soluzioni, l'utente potrà venire a conoscenza di informazioni tecniche, commerciali, finanziarie, operative e/o amministrative riservate e segrete (quali, a titolo esemplificativo e non esauritivo, dati personali, specifiche tecniche, schemi e configurazioni, codice sorgente e altro materiale relativi a prodotti, processi, marchi, brevetti o formule) di esclusiva proprietà e pertinenza di Progetti e Soluzioni.

L'organizzazione, per l'instaurazione di un rapporto di lavoro e/o per la corretta gestione del rapporto lavorativo con l'Utente, è tenuta ad entrare in possesso e a trattare dati, riferiti al dipendente/alla società ed eventualmente ai suoi familiari, qualificati come dati personali ai sensi delle norme vigenti in materia. A tal fine, il dipendente o la società dovranno sottoscrivere un'apposita informativa in cui sono esplicitati i loro diritti in materia.

Le informazioni appartenenti all'organizzazione, riservate o meno, classificate sulla base della PO-5.2-05 Policy di classificazione delle informazioni, devono essere usate dai dipendenti solo per gli scopi aziendali espressamente autorizzati.

È fatto specifico divieto di trasferire mediante qualsiasi mezzo (forum, chat, posta, telefono, rete, ecc...) informazioni relative alla società o a società ad essa collegate (fornitori, clienti, partner), senza l'approvazione preventiva del titolare dell'informazione e delle relative funzioni competenti.

Ove non strettamente necessario (e comunque previa approvazione del responsabile di funzione) si fa divieto di condividere informazioni con esterni, o personale di Progetti e Soluzioni non autorizzato. È fatta esplicita richiesta di far valere il **principio del buon senso e di riservatezza, limitando a quanto strettamente necessaria la divulgazione delle stesse**.

L'Utente non è autorizzato ad accedere, né a tentare l'accesso alle informazioni per le quali non ha alcun privilegio; è altresì **vietato tentare di procurarsi privilegi non concessi dal proprietario del dato**. Se per errore (ad esempio e-mail inviata ad un destinatario sbagliato) o a causa di un errato malfunzionamento del sistema, l'Utente dovesse entrare in possesso di informazioni di cui non è autorizzato, egli è tenuto a

 PROGETTI E SOLUZIONI	POLICY		PL-5.2-06	
	USER POLICY			Rev. 1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
	Pagina :			6 di 17

chiudere immediatamente il programma o/e distruggere l'informazione, comunicando l'accaduto al Responsabile per la Sicurezza delle Informazioni.

- L'organizzazione gestisce l'integrità e la disponibilità dei dati rilevanti ai fini aziendali tramite hard disk disponibili sui server e accessibili attraverso le specifiche **applicazioni WEB aziendali (Archimede, Mexal)**.
- I dati presenti nei dispositivi aziendali devono essere sincronizzati con il servizio **Google Drive**, che garantisce il servizio di backup e restore in caso di danneggiamento accidentale dei file sul PC.
- Gli utenti sono ritenuti responsabili della sicurezza dei dati aziendali e a mettere in atto ogni possibile cautela utilizzando tutte le modalità a loro disposizione, valutando ogni situazione di potenziale rischio con **senso di responsabilità**.
- I file contenenti informazioni particolarmente critiche (ad esempio, dati particolari di terze parti, specifiche tecniche relative a software proprietario di Progetti e Soluzioni, elenchi di password e in generale qualunque informazione che potrebbe cagionare danno all'azienda se rivelata all'esterno) devono essere conservate sui dispositivi personali esclusivamente in archivi criptati con il software KeePass.

Gli utenti che custodiscono informazioni critiche, nelle postazioni in dotazione, devono rispettare tutte le disposizioni previste per assicurare che queste informazioni non siano rese disponibili a persone non autorizzate, ovvero vengano smarrite o rubate (vedi gestione della propria postazione di lavoro e delle proprie credenziali di accesso)

Le informazioni riservate o contenenti dati personali (di altri dipendenti o di terzi) non possono essere portate fuori dai perimetri dell'organizzazione, attraverso alcun mezzo, senza previa ed esplicita autorizzazione.

Gli **smartphone, laptop, o altri strumenti portatili contenenti dati riservati non devono essere mai lasciati incustoditi**. L'Utente autorizzato a portare con sé i suddetti strumenti al di fuori del perimetro aziendale deve garantire una corretta gestione degli strumenti (es. non lasciandoli mai incustoditi nelle proprie auto, in luoghi pubblici, all'imbarco dei voli, ecc...).

Solo **previa autorizzazione della Direzione** o dell'interessato, la trasmissione dei dati personali deve essere attuata attraverso strumenti tecnologici adeguati, volti a garantirne la confidenzialità (es. cifratura del canale di comunicazione, cifratura del file contenente le informazioni da trasmettere, ecc...).

Le informazioni riservate non possono essere discusse o lette in luoghi pubblici come ristoranti, ascensori o mezzi di trasporto pubblico, senza le necessarie precauzioni. È altresì opportuno evitare di riferire tali informazioni per telefono, soprattutto in presenza di persone che non siano coinvolte nella materia trattata.

Gli utenti non possono effettuare modifiche sul livello di classificazione dei dati, se non espressamente autorizzati.

Gli utenti non possono distruggere o eliminare informazioni critiche per l'azienda, senza preventiva autorizzazione.

Gli utenti che vengono a conoscenza di **accessi non autorizzati da parte di terzi** ai dati aziendali, o ai dati personali degli utenti delle applicazioni WEB gestite da Progetti e Soluzioni, **devono informare tempestivamente il Responsabile della Sicurezza delle Informazioni** fornendo tutti i dettagli in proprio possesso per consentire la valutazione del danno.

4.1 CLAUSOLE CONTRATTUALI SULLA RISERVATEZZA DELLE INFORMAZIONI

I dipendenti che trattano dati di rilevanza strategica, in termini di business o continuità operativa, dovranno sottoscrivere delle clausole aggiuntive che definiscono con maggiore dettaglio le responsabilità in materia di riservatezza ed integrità (accordo di riservatezza).

5 MODALITÀ DI ACCESSO DEI DIPENDENTI E DEGLI OSPITI ALLE STRUTTURE

Il dipendente o la società con cui è stato sottoscritto un contratto di collaborazione che riceve un ospite esterno ne è responsabile dell'accompagnamento per tutta la durata della visita. Ciò è valido per gli uffici e soprattutto per le aree ad accesso riservato (locale server o locali contenenti dispositivi o informazioni classificate). Tale misura è necessaria al fine di ridurre le possibilità di commettere illeciti volti a recare danno all'organizzazione, o che gli ospiti vengano a conoscenza di attività, misure di sicurezza o informazioni non pubbliche relative a Progetti e Soluzioni.

 PROGETTI E SOLUZIONI	POLICY	PL-5.2-06		
	USER POLICY		Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
			Pagina :	7 di 17

Il dipendente o il collaboratore è tenuto, per quanto di sua pertinenza, a controllare l'accesso fisico agli uffici, locali riservati, e a tenere conto dei rischi che derivano dalla presenza di persone non autorizzate. Qualsiasi abuso in merito va tempestivamente segnalato al Responsabile per la Sicurezza delle Informazioni.

6 SICUREZZA DEI SISTEMI INFORMATIVI

L'uso degli strumenti informatici è limitato alle necessità aziendali e professionali di Progetti e Soluzioni e deve avvenire secondo le disposizioni indicate nella presente policy.

6.1 GESTIONE DELLA CREDENZIALI DI ACCESSO

Il Sistema Informativo Aziendale di Progetti e Soluzioni prevede **l'accesso tramite identificativo univoco (User-ID) e di una password necessari** a dimostrare la propria identità al sistema o all'applicazione a cui si sta effettuando l'accesso. Tali credenziali sono strettamente personali. **È vietato condividere le proprie credenziali, cederle ad altri o utilizzare credenziali di altri utenti.**

6.2 REGOLE DI UTILIZZO DELLE CREDENZIALI

- L'accesso agli applicativi di Progetti e Soluzioni prevede l'utilizzo di credenziali di accesso necessarie a dimostrare l'identità della persona incaricata alla lettura, modifica, cancellazione di informazioni.
- Le credenziali sono costituite da: **Username + Password + Token OTP** (One Time Password, quando previsto).
- Allo scopo di tutelare la sicurezza dei dati memorizzati negli applicativi occorre che le credenziali di accesso siano strettamente personali, assegnate nominalmente alle singole persone. Non è quindi consentita l'esistenza di credenziali che non soddisfino tale requisito.
- Durante una sessione di lavoro l'assegnatario non deve mai lasciare aperta la sessione rendendo accessibile l'applicazione, neppure in caso di breve allontanamento dal dispositivo.
- L'assegnatario è responsabile dell'utilizzo e della segretezza delle Credenziali di Accesso e si impegna ad informare tempestivamente l'Amministratore di Sistema (email a sysadmin@eusoftdesign.eu) in caso di uso non autorizzato, furto, smarrimento, malfunzionamento delle Credenziali di Accesso, manlevando Progetti e Soluzioni da ogni eventuale responsabilità al riguardo ed in generale da ogni e qualsiasi responsabilità relativa ad eventuali danni diretti o indiretti causati o subiti nell'utilizzo dell'applicazione per una scorretta custodia delle credenziali.

6.3 REGOLE DI UTILIZZO DELLE PASSWORD

La password inizialmente assegnata deve essere autonomamente modificata dall'assegnatario al primo accesso al sistema utilizzando le seguenti regole necessarie a rendere sicura una password:

- *Non utilizzare nomi noti, anche di fantasia (pippo, pluto, paperino, ecc...)*
- *Utilizzare password di almeno 12 caratteri*
- *Utilizzare una composizione di lettere maiuscole e minuscole, numeri e punteggiatura*
- *Cambiare spesso le password utilizzate, almeno ogni tre mesi*
- *Non appuntare la password su fogli, post-it o documenti informatici non criptati. Utilizzare il password manager KeePass*
- *Digitare la password al riparo da sguardi indiscreti*
- *Non utilizzare composizioni di lettere o numeri che siano riconducibili facilmente alla propria persona (ad esempio, date di nascita o altri eventi, nomi dei figli, del cane o del gatto, ecc.)*
- *Non comunicare a nessuno la password (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare).*

La password deve poi essere modificata periodicamente a cura dell'utente, sempre rispettando le regole sopra descritte, al fine di rendere più difficile l'identificazione da parte di malintenzionati.

6.4 TOKEN OTP SU GOOGLE AUTHENTICATOR (ONE TIME PASSWORD).

Quando previsto. Il dispositivo OTP Google Authenticator, da installare a cura dell'utente sullo smartphone aziendale (o in assenza, sullo smartphone personale), è uno strumento sicuro grazie al sistema One Time Password, che genera una password temporanea (pochi secondi), valida una sola volta per l'autenticazione

 PROGETTI E SOLUZIONI	POLICY	PL-5.2-06		
	USER POLICY		Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
			Pagina :	8 di 17

e non riutilizzabile. Ad incrementare il livello di sicurezza contribuisce l'associazione univoca al proprio dispositivo e l'impossibilità di duplicazione. Il Token OTP è intuitivo e semplice da utilizzare.

Funzionamento di Google Authenticator

Al primo accesso da parte dell'utente, il gestionale genererà un QR code e lo invierà all'email dell'utente. Aprire l'app Google Authenticator e inquadrare il QR code per associare lo smartphone in uso all'utenza. All'interno dell'app comparirà una riga riferita all'utente, con un codice a 6 cifre che si aggiornerà ogni 30 secondi. In fase di login, utilizzare il codice visualizzato (token OTP) in abbinamento ai propri nome utente e password per accedere al gestionale.

6.5 INTERNET

Internet è uno strumento messo a disposizione agli utenti dalla Direzione Aziendale per usi **esclusivamente professionali** (con le eccezioni indicate nelle pagine seguenti). **L'Utente si assume ogni responsabilità per un utilizzo improprio del servizio.**

Affinché sia garantita la tutela dell'Utente e dell'organizzazione che accede al servizio è necessario rispettare le seguenti regole:

- Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- **Non è consentito scaricare software gratuiti** (freeware e shareware) prelevati da siti Internet, se non espressamente autorizzato dalle strutture competenti (per conoscere quale software si è autorizzato a installare sul proprio PC, consultare il modulo Mod 630-02: Controllo software autorizzato). È proibito scaricare video, brani musicali, giochi e materiale coperto da diritto d'autore.
- **Non è consentito lo scambio (ad esempio Peer-to-Peer)** a qualsiasi titolo, anche se *non a scopo di lucro*, di materiale audiovisivo, cinematografico, fotografico, informatico, ecc., protetto da copyright.
- **Non è consentito effettuare ogni genere di transazione finanziaria** ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal proprio responsabile e con il rispetto delle procedure di acquisto aziendali.
- Tutte le azioni dell'Utente e tutti i dati riguardanti l'Utente possono essere oggetto di osservazione e di analisi da parte di terzi (siti visitati, messaggi scambiati, informazioni fornite tramite formati, dati raccolti, ecc.), allo scopo di determinare i suoi interessi e/o gli interessi dell'azienda, e potrebbero essere usati per comunicazioni commerciali o per altre finalità. **L'Utente a tale riguardo deve prendere tutte le precauzioni necessarie**, evitando altresì di registrarsi su siti commerciali, poco conosciuti, di dubbia credibilità.
- A scopo di statistiche, qualità del servizio e sicurezza, il **traffico Internet può essere controllato e possono essere fatte dai referenti tecnici di Progetti e Soluzioni** delle verifiche periodiche, entro i limiti di legge, volte ad accertare eventuali illeciti.
- **Non sono permesse la partecipazione a forum, l'utilizzo di chat line o di bacheche elettroniche**, anche utilizzando pseudonimi, se non per motivi professionali.
- **Tutti i file di provenienza incerta o esterna**, ancorché attinenti all'attività lavorativa, devono essere sottoposti al **controllo antivirus**.
- **Non è consentito scaricare e/o memorizzare file di grandi dimensioni**; eventuali necessità attinenti all'attività lavorativa, devono essere segnalate preventivamente a SysAdmin per essere autorizzate dalle strutture competenti, e comunque devono avvenire fuori dell'orario lavorativo.
- **Non è consentito connettere gli strumenti informatici aziendali (personal computer, palmari, ecc.) a reti esterne pubbliche (Internet) o private** (sistemi di altre società) né in LAN, né con strumenti wireless di qualsiasi genere, senza un'esplicita autorizzazione.
- L'Utente si impegna a non interferire volontariamente con il buon funzionamento dei sistemi informatici e di rete, avendo comunque la responsabilità di **segnalare tempestivamente la SysAdmin la presenza di attività sospette sui propri sistemi**, allo scopo di effettuare le opportune verifiche da parte del personale responsabile di gestire la rete.

 PROGETTI E SOLUZIONI	POLICY		PL-5.2-06	
	USER POLICY			Rev. 1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
	Pagina :	9 di 17		

- **È proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva di Gruppo Progetti e Soluzioni o che possa essere nocivo in qualsivoglia maniera. E' proibita qualsiasi attività (di trasmissione/download/salvataggio/connessione) che possa essere considerata come illegale, fraudolenta, spiacevole, di disturbo, offensiva, discriminatoria, diffamatoria.**

6.6 REGOLE DI UPLOAD SU FTP E MONITORAGGIO

- **Non è consentito effettuare l'upload di file di grandi dimensioni (es > 1GB) sulle aree FTP, senza avere prima informato di tale necessità SysAdmin in modo da prendere le eventuali precauzioni ed effettuare l'operazione senza influire in maniera dannosa sulle risorse di rete.**
- Al fine di prevenire la saturazione dei dischi remoti, il sistema effettua dei controlli automatici dell'uso dei dischi ogni ora.
- Se viene superata la soglia oraria stabilita nel documento **Mod.423-12 _Controllo Monitoraggio Capacità**, viene inviata una mail automatica a SysAdmin, che chiuderà temporaneamente il server e avvierà un'indagine.

6.7 FONTI DI INFORMAZIONI SU INTERNET

Generalmente non esiste un processo di qualità che attesta la veridicità delle informazioni che transitano sui siti Internet. È opportuno, dunque, che l'Utente, prima di impiegare le informazioni in un documento aziendale, consulti altre fonti più attendibili.

Prima di utilizzare una fonte, una informazione, testi o immagini, all'interno di propri lavori, è opportuno richiedere l'autorizzazione della fonte, citandola esplicitamente nel proprio documento (*come previsto dalla legge sul copyright - diritto d'autore*).

6.8 INTRANET

L'accesso all'intranet aziendale ed ai relativi servizi (portali interni, repository documentali, posta elettronica, etc.) è possibile solo tramite **credenziali personali ed individuali, conseguentemente non possono essere condivise o cedute a terzi**.

L'utilizzo delle informazioni o della **documentazione acquisita tramite l'intranet aziendale è classificata ad "uso interno"**, pertanto l'utilizzo è limitato alla sola attività lavorativa e sempre nel rispetto della legge sul copyright.

L'Utente deve tenere un comportamento politicamente corretto nell'utilizzo della rete aziendale. A tal riguardo, non deve effettuare nessun tipo di attività volta ad eludere o compromettere i meccanismi di protezione dei sistemi informatici. Non è permesso intercettare (tecnicamente *sniffare*) pacchetti in transito in rete e destinati ad altri host per individuare informazioni o credenziali di accesso. Così come è vietato l'utilizzo di qualsiasi tecnica o strumento per la violazione dei sistemi o delle reti (sia interne che esterne).

È opportuno che gli utenti non condividano in rete file, cartelle, programmi, senza preventiva autorizzazione dal proprio responsabile e dai gestori del Sistema Informativo Aziendale.

6.9 POSTA ELETTRONICA

La posta elettronica aziendale è uno strumento messo a disposizione agli utenti dalla Direzione Aziendale per usi esclusivamente professionali. **L'Utente si assume ogni responsabilità per un utilizzo improprio del servizio di posta elettronica.**

L'utenza di posta elettronica è strettamente personale ed è pertanto responsabilità dell'Utente garantire la riservatezza delle credenziali di accesso al servizio.

Per una corretta fruizione del servizio di posta elettronica, che tuteli l'Utente e l'Organizzazione, devono essere rispettate le seguenti regole:

- L'uso per fini personali dell'account di mail aziendale non è consentito in nessun caso. In alcuni casi particolari, inoltre, su esplicita richiesta dell'Autorità Giudiziaria competente, le e-mail memorizzate nei server di Progetti e Soluzioni potrebbero essere eventualmente divulgate o rese note a terzi.
- L'utente deve attivare l'autenticazione a due fattori sul proprio account di posta aziendale. Per effettuarlo deve accedere via web alla propria casella di posta su Google Workspace, cliccare sul proprio nome utente in alto a sinistra, quindi sul pulsante *Gestisci il tuo account Google*, e infine sulla scheda *Sicurezza*. È possibile configurare come secondo fattore di accesso il proprio cellulare

 PROGETTI E SOLUZIONI®	POLICY		PL-5.2-06	
	USER POLICY			Rev. 1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
	Pagina :	10 di 17		

aziendale o personale, oppure l'app Google Authenticator. In caso di difficoltà, chiedere supporto all'amministratore di sistema (sysadmin@eusoftdesign.eu).

- **Non è consentito inviare o memorizzare messaggi di natura oltraggiosa**, volgare e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- **Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mailing-list**, salvo diversa ed esplicita autorizzazione. L'iscrizione ad una mailing list o a servizi simili (chat, forum, ecc.) è consentita solo se funzionale all'attività aziendale.
- **Non è, altresì, consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per inviare messaggi di tipo umanitario, sociale o di solidarietà**, salvo diversa ed esplicita autorizzazione rilasciata dal proprio responsabile gerarchico.
- **È vietato l'usa della posta elettronica per ricevere, memorizzare o spedire materiale che violi il copyright**, il marchio o altre leggi sul diritto d'autore (cfr. Leggi sul diritto d'autore DL 68/2003).
- L'Utente deve ricordare che ogni comunicazione effettuata tramite posta elettronica può essere intercettata, letta, copiata, modificata e inviata ad un altro indirizzo. Di conseguenza, **nessuna informazione riservata deve essere trasmessa direttamente tramite e-mail, a meno che venga trasmessa attraverso una forma cifrata autorizzata**. Le informazioni sensibili per l'azienda devono essere scambiate all'interno dell'azienda utilizzando i gestionali appropriati (Archimede). Comunque, prima di inviare qualsiasi tipo di informazione e/o documenti di proprietà di Progetti e Soluzioni tramite posta elettronica, l'Utente deve essere:
 - Consapevole dell'impatto che l'intercettazione di tali informazioni potrebbe avere sull'organizzazione.
 - Verificare che non vi siano disposizioni esplicite, per la natura dell'informazione/documento, che prescrivano una diversa forma, più sicura, di trasmissione.
- È opportuno assicurarsi che il destinatario dell'e-mail sia effettivamente quello desiderato. Nel caso si commetta un errore nella spedizione di una e-mail occorre contattare il destinatario, chiedendogli di cancellare il messaggio.
- Ogni e-mail inviata deve contenere, come nota finale allegata in automatico, un'adeguata informativa relativa alle informazioni confidenziali. (Esempio: *Questa e-mail, nonché qualsiasi file allegato alla presente, è destinata esclusivamente ai destinatari indicati in indirizzo o a chi sia stato da essi autorizzato. Se questa e-mail è stata ricevuta per errore, si chiede cortesemente di avvisare immediatamente il mittente e di distruggere permanentemente il messaggio e i relativi allegati.*)
- È necessario **fare attenzione alla posta ricevuta**. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da *codici maligni*, occorrerà cancellare i messaggi senza aprirli. In ogni caso è **obbligatorio controllare tramite il software antivirus tutti file in allegato prima del loro utilizzo**. È vietato eseguire il download di file eseguibili senza preventiva richiesta da inviare a SysAdmin, che effettuerà le relative verifiche con gli enti preposti.
- È necessario prestare attenzione ai **tentativi di phishing**, in cui malintenzionati si fingono persone note per chiedere di anticipare consistenti somme in denaro. In particolare, controllare:
 - **L'indirizzo mail del mittente**. Il malintenzionato potrebbe usare nomi noti, inviando l'email da un indirizzo diverso. Il campo "DA" delle mail contiene sempre due elementi, il nome e l'indirizzo: controllarli entrambi per verificare che siano congruenti con l'identità che il mittente dichiara;
 - **Il numero di telefono eventualmente utilizzato**. In genere per questo tipo di raggiri vengono utilizzati numeri non italiani, per limitare le possibilità di intervento delle forze dell'ordine. Il prefisso internazionale italiano è +39.
 - **Il tono e la natura delle richieste**. I malintenzionati hanno sempre fretta e usano toni perentori. La richiesta dei truffatori sarà quasi sempre di convertire dei soldi in buoni omaggio che, una volta riscattati, non sono più rintracciabili.

 PROGETTI E SOLUZIONI	POLICY		PL-5.2-06	
	USER POLICY			Rev. 1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
	Pagina :	11 di 17		

- **Attenzione ad allegati e link.** Evitare sempre di aprire contenuti provenienti da fonti sospette. Anche qualora il link o allegato sia stato inviato da un contatto verificato, meglio accertarsi che il mittente lo abbia inviato volontariamente e che non si tratti di un messaggio automatico inviato a causa di un dispositivo infetto o un account compromesso.
 - **Attenzione alle richieste di credenziali.** Spesso i malintenzionati inviano mail che simulano quelle di servizi noti, chiedendo di collegarsi a un link e inserire le proprie credenziali. In questo modo, riescono a carpire le credenziali e ottenere l'accesso all'account del malcapitato. Prestare attenzione all'url del link presente in queste mail. In generale, comunque, nessun servizio serio invia richieste di inserimento credenziali di questo tipo.
- Quando possibile, inviare sempre gli allegati in un formato compresso (*.zip *.rar) ed **evitare l'invio di file superiori ai 5 MB. È eccezionalmente possibile previa preventiva richiesta tramite SysAdmin.**
- Non spedire ed in ogni caso **non partecipare a “catene di S. Antonio”**, poiché si configurano come atti di “spamming” e la diffusione incontrollata di tali messaggi potrebbe impattare sull'efficienza del sistema di posta. Per limitare il fenomeno dello spamming è opportuno anche evitare di diffondere il proprio indirizzo e-mail aziendale attraverso siti, forum, chat o quanto altro ritenuto non affidabile e pertinente alla propria attività lavorativa.
- **L'Utente è tenuto a mantenere in ordine la sua casella di posta**, cancellando documenti inutili ed e-mail non necessarie, in modo tale da razionalizzare l'impiego di risorse.
- Le e-mail trasmesse da un'entità delle società di Progetti e Soluzioni generalmente possono essere considerate come "sicure", anche se si invita a fare sempre le dovute verifiche del caso. Ad esempio, in caso di richiesta di invio di denaro o di invio di credenziali di accesso, effettuare prima una verifica telefonica con il mittente della comunicazione.
- Il tono, la presentazione e lo stile della posta elettronica devono riflettere l'immagine aziendale.
- In caso di assenza prolungata, nei casi in cui si renda necessario trasferire i messaggi ricevuti sulla casella di posta di un utente, è necessario che il trasferimento venga autorizzato dal proprio responsabile, che provvederà a richiedere la configurazione del trasferimento a SysAdmin. Tale operazione, in accordo con le norme sulla privacy, deve essere preventivamente autorizzata dall'utente titolare della casella di mail.
- In caso di cessazione del rapporto di lavoro, nei casi in cui l'archivio email del dipendente possa essere un valore per l'azienda, la Direzione Generale può chiedere a SysAdmin di mantenere copia dell'intero archivio mail dell'ex dipendente. Deve essere cura del dipendente, prima della chiusura del rapporto di lavoro, la cancellazione di qualunque messaggio ricevuto a titolo personale e non lavorativo. L'Utente sottoscrivendo il presente documento accetta fin da ora che, a conclusione del rapporto di lavoro, l'archivio delle proprio email potrà essere oggetto di attività di monitoraggio e/o di salvataggio (*back-up*).
- Eventuali mail inviate agli indirizzi degli ex-dipendenti dopo la cessazione del rapporto di lavoro, come da normativa vigente, non saranno conservate né inoltrate a nessuno. Sarà attivato un risponditore automatico che informerà lo scrivente che la casella non è più attiva e sarà data indicazione di un indirizzo alternativo da utilizzare per la gestione della comunicazione. Il risponditore sarà attivo per un periodo di tempo limitato, a seconda del ruolo ricoperto al dipendente e dal livello di interazione di tale ruolo con l'esterno.

6.10 USO PERSONALE

Internet e la posta elettronica sono servizi che Progetti e Soluzioni fornisce ai propri utenti per scopi aziendali.

Sarà tollerato l'uso, esclusivamente occasionale e fortuito, di Internet per scopo personale solo se questo non avrà un effetto negativo sul livello della performance dei sistemi o sull'attività lavorativa generale. Sta all'Utente rispettare le regole del buonsenso e valutare il limite ragionevole di questo uso.

 PROGETTI E SOLUZIONI	POLICY			PL-5.2-06	
	USER POLICY			Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato	Pagina : 12 di 17

6.11 ACCESSO REMOTO

L'accesso remoto all'intranet aziendale deve avvenire unicamente con i PC dati in dotazione dall'organizzazione o, negli altri casi, da un personal computer che garantisca una configurazione conforme alle disposizioni di questo regolamento.

6.12 TELELAVORO E SMART WORKING

Il telelavoro in generale non è una modalità lavorativa consentita in Progetti e Soluzioni, fatto salvo per le società con le quali è stato sottoscritto un contratto di collaborazione, le quali ovviamente svolgono la loro attività nelle rispettive sedi. Il telelavoro è consentito, senza necessità di ulteriori autorizzazioni da parte della Direzione, ai dipendenti che risiedono e svolgono le proprie funzioni lontano dalle sedi aziendali.

Lo **smart working** può essere utilizzato in accordo con le leggi e i contratti nazionali in vigore, previa accordo individuale tra il lavoratore e l'azienda, o per eventuale temporanea indisponibilità delle strutture aziendali (ad esempio, per pandemie, ristrutturazioni, disinfezioni, assenza prolungata della connettività Internet, ecc.) gestita attraverso i piani di continuità di riferimento.

Nel caso in cui **l'Utente** lavori da casa a vario titolo, in aggiunta a tutte le norme già elencate precedentemente, deve rispettare anche le seguenti norme di comportamento:

- La connessione a Internet utilizzata deve essere sicura. In caso di rete domestica LAN, questa deve essere interamente contenuta nel perimetro domestico, non accessibile dall'esterno e protetta da un firewall. In caso di rete WiFi, questa deve essere dotata di chiave di sicurezza WPA2; il WPA è fortemente sconsigliato, il WEP è assolutamente vietato.
- Mentre **l'Utente** lavora da casa, deve prestare attenzione a non lasciare i dispositivi aziendali accessibili per l'utilizzo da parte di familiari, conviventi od ospiti non autorizzati all'accesso dei dati. A tale proposito, valgono le disposizioni relative a clear desk policy, clear screen policy e protezione con password del dispositivo già esposte nel resto del presente documento.
- L'utilizzo a fini personali delle attrezzature fornite, anche nei periodi di lavoro da casa, deve sempre rispettare le regole esplicitate nel resto del presente documento.

7 UTILIZZO DELLE POSTAZIONI DI LAVORO

La Postazione di Lavoro (PdL) è costituita dall'insieme di componenti hardware e software forniti all'utente dall'azienda o di proprietà dell'utente ed autorizzate dall'Azienda, al fine di svolgere le proprie attività lavorative, in quanto consente l'accesso al complesso dei sistemi e servizi resi disponibili dall'azienda.

La PdL deve essere sempre utilizzata per finalità lecite, rispettando le normative aziendali e in ottemperanza alle disposizioni legislative vigenti.

Pertanto, la PdL non deve essere utilizzata: con modalità che possano provocare malfunzionamenti o danneggiamenti del sistema informatico; arrecare danni ad altri utenti; a fini di lucro o commerciali; per effettuare scanning e campionamento dell'attività dei sistemi o della rete aziendale; per promuovere spamming e hoax (bufala); per accedere a siti e materiali i cui contenuti e scopi siano lesivi dell'etica e della comune morale.

Di seguito sono riportate le istruzioni operative per il corretto e sicuro utilizzo delle risorse hardware e software che costituiscono la PdL e dei sistemi e servizi informatici a cui l'utente può accedere attraverso la PdL stessa.

7.1 HARDWARE

L'Utente è responsabile della propria postazione di lavoro, assegnata dall'Azienda e deve custodirla con diligenza, segnalando eventuali furti, danneggiamenti o smarrimenti. L'elenco dei dispositivi hardware assegnati all'Utente è disponibile su Archimede, nella scheda Assegnazioni relativa all'Utente aziendale.

In assenza momentanea dell'Utente, l'apparecchiatura portatile (laptop, smartphone, chiavette, hard-disk esterni, ecc.) deve essere custodita in luoghi sicuri contro il furto (es. in armadietti chiusi a chiave, etc.).

 PROGETTI E SOLUZIONI	POLICY			PL-5.2-06	
	USER POLICY			Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato	Pagina : 13 di 17

Se un personal computer, o qualsiasi altro dispositivo, viene portato fuori dell'edificio aziendale, devono essere prese tutte le precauzioni perché non si smarrisca, venga danneggiato o rubato.

A tal proposito l'Utente deve prestare assoluta attenzione nel non lasciare mai incustodita alcuna strumentazione o documentazione aziendale, nella propria autovettura, piuttosto che in luoghi pubblici, o non sicuri.

L'Utente deve informare subito i suoi superiori di qualsiasi danno, furto o perdita di apparecchiatura, software e/o informazioni che gli sono state affidate.

L'Utente non deve modificare la configurazione hardware della postazione di lavoro (fissa e/o mobile), aggiungendo o rimuovendo componenti, rispetto allo standard definito e fornito dall'azienda. Qualora sia necessario può richiedere, previa verifica da parte del proprio responsabile, l'aggiornamento della propria configurazione hardware rivolgendosi alle funzioni competenti.

L'utente non deve mai disattivare la password di accensione sulla propria postazione di lavoro.

Non è permesso sottrarre dispositivi, apparecchiature e/o informazioni, in esse contenute, di proprietà dell'azienda.

La disponibilità di informazioni complete circa la configurazione e la consistenza delle PdL consente di monitorare costantemente la presenza di situazioni di rischio legate alla presenza di vulnerabilità e di individuare gli aggiornamenti di sicurezza che consentono di ridurre tali rischi.

Per queste ragioni l'utente in qualità di responsabile dell'uso e della conservazione delle risorse informatiche a lui assegnate, è tenuto a prestare la massima collaborazione sia alle attività di censimento ed inventario delle risorse hardware e software, sia alle attività di aggiornamento di tali risorse.

7.2 SMARTPHONE

Di seguito le regole per gli utenti a cui è stato assegnato uno smartphone aziendale:

- Utilizzare una password per l'accesso allo smartphone (PIN, percorso, impronta digitale)
- Non lasciare mai il dispositivo incustodito (in auto, sale riunioni, ristoranti ecc.)
- Utilizzare i server forniti dall'azienda per conservare i documenti importanti (ad esempio, Google Drive, Archimede)
- In caso di furto del dispositivo, cancellare da remoto tutti i dati del dispositivo. Poiché i contatti, l'agenda, l'email e i file su drive sono sincronizzati via web tramite l'account Google, è necessario rimuovere tutti i dati dal dispositivo appena possibile. A tal fine, è necessario seguire la seguente procedura:

1. **Una Tantum.** Sul dispositivo Android, abilitare le opzioni per:

- Trova il mio dispositivo
- Geolocalizzazione

Come descritto nel seguente articolo:

<https://support.google.com/accounts/answer/3265955>

2. **Nel caso in cui il dispositivo Android venga smarrito o rubato,** collegarsi da browser usando il proprio account GSuite al seguente URL:

<https://www.google.com/android/devicemanager>

3. Verificare la posizione del dispositivo sulla mappa e usare una delle 3 opzioni proposte nel menù a sinistra (**Riproduci audio**, **Blocca il dispositivo** o **Resetta il dispositivo**), a seconda della gravità della situazione.

- Non installare mai app provenienti da fonti sospette: installa solo app necessarie per il lavoro, presenti sul Google Play Store, che abbiano almeno 50.000 utenti e che non abbiano evidenti problemi di sicurezza evidenziati nei commenti.

 PROGETTI E SOLUZIONI®	POLICY		PL-5.2-06	
	USER POLICY			Rev. 1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato
	Pagina :			14 di 17

7.3 STRUMENTI DI SUPPORTO

Gli strumenti di identificazione/autenticazione (lettori di *fingerprint*, smart card, badge, ecc.) sono strettamente personali e non devono mai, per nessun motivo, essere ceduti o comunicati a terzi.

L'utilizzo di supporti di memoria rimovibili (CD, chiavi USB, Hard Disk rimovibili, ecc.) **deve essere limitato il più possibile**. Le informazioni riservate e i documenti contenenti dati personali devono essere scambiati o trasferiti esclusivamente tramite Internet sui canali autorizzati dall'azienda (Google Drive e gestionali aziendali).

Nel caso in cui si rendesse indispensabile il trasporto di supporti di memoria contenenti dati personali, particolari, giudiziari o strategici per l'organizzazione, i supporti devono essere crittografati utilizzando il software VeraCrypt prima del trasporto. Tali supporti devono essere conservati in luoghi protetti (ad esempio, armadi e cassettiere chiusi a chiave), cancellati quando i dati non sono più necessari o distrutti, in modo irreversibile, nel caso non fosse possibile cancellarli. La cancellazione o la distruzione devono essere eseguite dall'Amministratore di Sistema oppure da un centro qualificato che rilasci apposita documentazione attestante la distruzione del supporto. In nessun caso il dipendente dovrà procedere in autonomia alla distruzione di supporti.

Nei casi in cui il trasporto non possa essere effettuato da personale interno di Progetti e Soluzioni, esso deve essere affidato esclusivamente a corrieri qualificati dalla direzione (rif. MO-8.4-01 Albo fornitori).

7.4 DISMISSIONE E RIUSO DEI DISPOSITIVI

Quando l'utente riconsegna un dispositivo per sostituzione o per fine del rapporto di lavoro, deve preventivamente provvedere a:

- Eliminare dal dispositivo eventuali dati personali archiviati;
- Rimuovere eventuali blocchi biometrici (ad esempio, impronta digitale);
- Impostare sul dispositivo una password temporanea, da comunicare al proprio responsabile alla restituzione del bene.

Prima che i dispositivi muniti di disco di archiviazione possano essere riutilizzati internamente, i dati precedentemente presenti devono essere cancellati in modalità sicura con il supporto di SysAdmin. A questo fine, SysAdmin dovrà provvedere a ripristinare il dispositivo alle impostazioni di fabbrica, **selezionando l'opzione di rimuovere tutti i dati in modalità sicura (*Rimuovi tutto*)**.

Nel caso i cui dispositivi non siano riutilizzabili, le unità di archiviazione devono essere distrutte fisicamente, utilizzando un martello o un trapano, oppure avvalendosi del supporto di ditte specializzate. I dispositivi devono poi essere smaltiti a norma di legge.

7.5 SOFTWARE

È opportuno, per garantire la sicurezza della propria postazione di lavoro e del sistema informativo di Progetti e Soluzioni, che l'Utente segua delle semplici regole:

- I dischi delle postazioni di lavoro sono crittografati tramite software BitLocker, al fine di proteggerne i contenuti in caso di smarrimento del dispositivo. È fatto divieto agli utenti di disattivare la crittografia sui dispositivi.
- Si fa divieto assoluto di fare il download, da Internet o provenienti da soggetti esterni all'organizzazione e di installare software non autorizzato (*anche se freeware*) sul personal computer. È dunque vietata l'installazione di qualsiasi prodotto che non sia:
 - Stato preventivamente autorizzato (vedere elenco software autorizzato, Mod 630-02)
 - Licenziato a Progetti e Soluzioni
- L'Azienda acquista le licenze d'uso del software per i computer da varie Società esterne. È soggetta a limitazioni nell'utilizzo di tali programmi e, a meno di una specifica autorizzazione concessa dallo sviluppatore del software, non ha il diritto, e con essa i propri utenti, di riprodurlo, salvo che per motivi di salvataggio (opportunamente documentati).
- Per quel che riguarda le applicazioni Client/Server e in rete, i dipendenti dell'Azienda sono tenuti a utilizzare il software solo entro i limiti specificati nei contratti di licenza.

 PROGETTI E SOLUZIONI	POLICY			PL-5.2-06	
	USER POLICY			Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato	Pagina : 15 di 17

- L'Utente deve aderire al programma di conformità alla legge sul copyright. Pertanto, ciò impone il divieto di riprodurre il software attraverso qualsiasi mezzo, di trasferirlo su una stazione di lavoro diversa da quella autorizzata, e di rivelare il software a parti esterne senza il consenso dell'organizzazione.
- Non è consentito riprodurre, adattare, trasformare, distribuire software in licenza d'uso aziendale.
- Secondo la legge sul copyright, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente sia penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione.
- L'Azienda non transige sulla duplicazione illegale del software e i dipendenti che fanno, acquisiscono o usano copie non autorizzate del software per i computer subiranno le sanzioni disciplinari previste caso per caso. Nei casi più gravi la sanzione può arrivare anche al licenziamento.
- È assolutamente vietato utilizzare e/o installare software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici (a titolo esemplificativo: programmi di recovery password, cracking, sniffing, spoofing, serial codes, ecc), a meno che l'attività non rientri in azioni autorizzate di penetration test/vulnerability assessment.
- È proibita ogni attività realizzata per violare o per collaudare la sicurezza del sistema, salvo autorizzata esplicita da parte delle funzioni aziendali preposte (Responsabile per la Sicurezza delle Informazioni, gestore Sistema Informativo, ecc).
- La manutenzione software deve essere fatta solo dal personale autorizzato e competente. Pertanto, si raccomanda a ciascun Utente di rivolgersi sempre a Sysadmin (sysadmin@eusoftdesign.eu).
- Nel caso in cui l'Utente venga a conoscenza di una qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi non deve assolutamente sfruttarla per commettere azioni illecite o non autorizzate, bensì deve tempestivamente informare la funzione sicurezza.
- È fatto specifico divieto di modificare gli standard di configurazione del proprio PC. Essi rispondono a criteri stabiliti dall'Organizzazione e la loro alterazione può generare problemi nella gestione dei software e negli interventi manutentivi. In tale ottica le direttive impartite dai Sistemi Informativi e dalla Sicurezza sono vincolanti.
- In caso di necessità di software, rivolgersi, per qualsiasi richiesta, solo alla struttura di help desk di riferimento che valuterà il rilascio del software richiesto in conformità alle regole aziendali in vigore e, se necessario, sottoporrà la richiesta all'attenzione del Responsabile per la Sicurezza delle Informazioni;
- Si raccomanda di tenere il sistema operativo del proprio dispositivo sempre aggiornato con le patch di sicurezza rilasciate da Microsoft.

7.6 ANTIVIRUS

Su ogni personal computer e smartphone deve essere installato il software antivirus standard aziendale, correttamente configurato ed aggiornato; è vietato disabilitare o inibire il corretto funzionamento del software anti-virus.

L'Utente deve accertarsi che, sulla propria postazione di lavoro, il software antivirus aziendale sia sempre aggiornato e funzionante, secondo le modalità stabilite dalle apposite procedure.

È vietato disattivare il software antivirus o modificarne la configurazione, disabilitare o disattivare i meccanismi di notifica automatica degli eventi e di segnalazione degli allarmi.

Qualora per la propria postazione di lavoro non esista un software antivirus rispondente alle norme, o non sia possibile installare correttamente il software antivirus Aziendale, l'Utente dovrà informare immediatamente il suo Responsabile. **L'Utente non può installare in autonomia altri software antivirus**.

Ogni Utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio **non aprire mail o relativi allegati sospetti, non navigare su siti non professionali o di dubbia integrità**, ecc.)

Prima di caricare un qualunque tipo di dato o programma da un supporto esterno (CD, DVD, penna USB, ecc.) gli utenti devono **procedere alla scansione del supporto utilizzando l'antivirus** messo a

 PROGETTI E SOLUZIONI	POLICY			PL-5.2-06	
	USER POLICY			Rev.	1
	<input type="checkbox"/> Pubblico	<input checked="" type="checkbox"/> Interno	<input type="checkbox"/> Limitato	<input type="checkbox"/> Riservato	Pagina : 16 di 17

disposizione dall'Azienda. Nel caso venga rilevato un virus non eliminabile dal software antivirus, l'Utente non deve utilizzare il dispositivo infetto.

Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, l'Utente deve immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto a **SysAdmin per le necessarie verifiche da parte delle funzioni competenti**.

Gli utenti non possono rimuovere virus con azioni personali, ma devono avvalersi dell'assistenza necessaria, attenendosi alle modalità stabilite dalle apposite procedure di gestione degli incidenti; ad operazione ultimata, devono accertarsi dell'eliminazione del virus e della riusabilità della postazione di lavoro.

Per installare l'antivirus aziendale sul proprio smartphone assegnato, seguire la seguente procedura (**da eseguire a cura e responsabilità di ciascun Utente**):

- Scaricare **GravityZone Mobile Client** da Google Play (esattamente l'app descritta, non altre app di Bitdefender), avviarla e configurare i parametri come segue:
 - Server: 88.80.149.44:8443
 - Token: contattare SysAdmin per ottenere il proprio token personale
 - Premere il tasto **Activate**, quindi selezionare **Trust**
 - Seguire le istruzioni a schermo per attivare la "modalità amministratore". Questa modalità consente all'amministratore di sistema di effettuare operazioni drastiche sul dispositivo quali la cancellazione dei dati e il blocco del telefono. Queste funzionalità sono utili in caso di furto o smarrimento del telefono e non saranno utilizzate in altre occasioni
- Inviare una mail all'amministratore di sistema per notificare l'avvenuta installazione

8 CONTROLLO E MONITORAGGIO DELLE RISORSE

Progetti e Soluzioni periodicamente procederà, nel rispetto delle garanzie di tutela dei dati personali, previste dal Testo Unico D.Lgs. 196/2003 e dal Regolamento UE n. 679/2016 (GDPR), ad un controllo quantitativo dell'utilizzo della rete, dei PC e della posta elettronica per verificarne un uso equilibrato e conforme all'attività ed alle politiche aziendali.

In particolare, controlli periodici possono essere effettuati su:

- Il volume dei messaggi scambiati
- Il formato dei file allegati
- La durata dei collegamenti ad Internet (globale, per funzione, per utenti)
- I siti visitati più frequentemente (globale, per funzione, per utenti)
- Le informazioni raccolte dai dispositivi di sicurezza (Firewall, Antivirus, IDS, ecc.) per rilevare e contrastare situazioni di illecito, ai sensi della L. 547/93 in materia di criminalità informatica.

Il monitoraggio non è finalizzato al controllo delle attività degli utenti (salvo eventuale esplicita richiesta in tal senso da parte delle Autorità competenti). Le informazioni raccolte consentono un controllo dell'efficienza e dell'utilizzo corretto delle risorse informatiche aziendali e del network.

I dati sopra descritti sono acquisiti in forma **anonima** e quindi non riconducibili all'identità del singolo Utente. I dati sono archiviati, con le misure di sicurezza opportune, nei limiti sanciti dal Regolamento UE sulla privacy (679/2016, GDPR) e le norme antiterrorismo (D.Lgs. 144/05), fatto salvo eventuali esplicite richieste delle Autorità competenti.