CODICE SULL'UTILIZZO AMMESSO DELLE DOTAZIONI INFORMATICHE E TELEMATICHE "Codice ICT"

2	**20.10.2025**	Aggiornamento GDPR e UNI CEI ISO/IEC 27001:2024	
1	**28.12.2013**	Adeguamento a modifica organo amministrativo	
0	**21/12/2011**	Emissione del documento	
Revisione	**data**	**Motivazione**	**Firma AD**

CODICE SULL'UTILIZZO AMMESSO DELLE DOTAZIONI INFORMATICHE E TELEMATICHE

Sommario

1 INTRODUZIONE 4
1.1 Scopo 4
1.2 Applicabilità 4
1.3 Riferimenti 4
2 FINALITÀ 4
3 DESTINATARI 5
4 RESPONSABILITÀ 5
4.1 Responsabilità degli Utenti Individuali (A.5.2, A.5.4, A.5.11) 5
4.2 Uso professionale (A.5.10, A.5.32) 5
4.3 Protezione contro furti e danneggiamenti (A.7.3, A.7.8, A.7.9, A.7.13) 5
4.4 Riservatezza e protezione del sistema e dei dati (A.5.15, A.5.12, A.5.13, A.5.33, A.5.34) 6
4.5 Politiche di Clear desk e Clear Screen (A.7.7, 27018 A.11.7) 6
4.6 Integrità e disponibilità dei dati (cartelle di rete) (A.8.13, A.8.14, A.5.33) 6
4.7 Utilizzo strumenti informatici (A.5.10, A.8.19, A.8.18) 7
Policy BYOD – Bring Your Own Device 8
(A.6.7, A.7.9, A.8.1, 27018 A.11.5) 8
A. Scopo 8
B. Ambito di applicazione 8
C. Requisiti minimi dei dispositivi 8
D. Sicurezza e protezione dei dati 8
E. Accesso e utilizzo 8
F. Privacy dell'utente 8
G. Responsabilità 8
H. Sanzioni 8
I. Accettazione 8

4.8 Credenziali di accesso (A.5.16, A.5.17, A.8.5) 9
4.9 Personal Computer/portatile (A.7.8, A.7.9, A.8.1, A.8.23, A.8.24) 9
4.10 Internet (A.5.14, A.8.20, A.8.21, A.8.22, A.8.23) 10
4.11 E-mail (A.5.14, A.5.33, A.5.34) 11
4.12 Uso personale (A.5.10) 12
4.13 Uso condiviso (A.5.15) 13
4.14 End user computing (A.8.26, A.8.13, A.8.33) 13
4.15 Cloud e backup (A.5.23, A.8.13, 27018 A.11.3) 13
4.16 Controlli e monitoraggio delle risorse (A.8.15, A.8.16, A.8.17, 27017 A.12.4.5) 13
4.17 Software (A.8.19, A.8.18, A.5.32) 14
4.18 Limitazione all'utilizzo di sistemi di crittografia (A.8.24) 15
5 VIOLAZIONE (A.6.4, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28) 15
6 FORMAZIONE E CONSAPEVOLEZZA (A.6.3, A.5.36) 15
7 SEZIONE NUOVA – Segregazione dei compiti (A.5.3) 15
8 SEZIONE NUOVA – Contatti con Autorità e gruppi di interesse; Threat Intelligence (A.5.5, A.5.6, A.5.7) 16
9 SEZIONE NUOVA – Inventario degli asset (A.5.9) 16
10 SEZIONE NUOVA – Verifica indipendente della sicurezza e conformità (A.5.35, A.5.36) 16
11 SEZIONE NUOVA – Uso della crittografia (A.8.24) 16
12 SEZIONE NUOVA – Classificazione ed etichettatura delle informazioni (A.5.12, A.5.13) 16
13 APPENDICE A – Gestione degli incidenti di sicurezza 17
14 APPENDICE B – Ciclo di vita delle utenze e riesami degli accessi 17
15 APPENDICE C – Data Loss Prevention e supporti rimovibili 17
16 APPENDICE D – Fornitori e supply chain 17
17 APPENDICE E – Sicurezza fisica e dei locali 18
18 APPENDICE F – Logging, monitoraggio e sincronizzazione oraria 18
19 APPENDICE G – Sicurezza e segregazione di rete 18
20 APPENDICE H – Continuità ICT e prove di ripristino 18
21 APPENDICE I – Screening pre-assunzione e cambi ruolo 18
22 APPENDICE L – Change management, dati di test e audit-testing 19

1 INTRODUZIONE

1.1 Scopo

Il presente documento ha lo scopo di definire le regole di comportamento per l'utilizzo delle risorse ICT aziendali, garantendo sicurezza, conformità normativa e protezione del patrimonio informativo.

1.2 Applicabilità

Il presente codice si applica a dipendenti, collaboratori, consulenti, visitatori e chiunque utilizzi risorse ICT di proprietà o in uso presso EURELETTRONICA ICAS srl.

1.3 Riferimenti

- Regolamento UE 2016/679 (GDPR)
- D.Lgs. 196/2003 aggiornato
- Linee guida del Garante Privacy
- Normativa sulla sicurezza informatica e cybercrime
- UNI CEI ISO/IEC 27001:2024 (i paragrafi riportano tra parentesi i riferimenti ai punti di controllo dell'allegato A della ISO27001)

2 FINALITÀ

- Proteggere disponibilità, integrità e riservatezza delle informazioni aziendali
- Prevenire comportamenti che possano compromettere la sicurezza dei sistemi
- Promuovere una cultura della sicurezza informatica tra tutti gli utenti

.

Il presente Codice di Condotta Informatica e Telematica è letto e sottoscritto dai destinatari indicati. L'utilizzo degli strumenti informatici aziendali da parte degli utenti non può avvenire senza aver preventivamente ricevuto e recepito le prescrizioni e le indicazioni ivi contenute.
Il presente Codice di Condotta Informatica è applicabile a tutto il personale della EURELETTRONICA ICAS srl, ai suoi consulenti, visitatori e quanti altri si trovassero a dover utilizzare le dotazioni ICT messe a disposizione dalla EURELETTRONICA ICAS srl.

Per dotazione ICT si intende qualsiasi risorsa informatica e/o telematica (es.: computer, software, rete, utenza, file, cartella di rete, telefono cellulare, modem, …) che la EURELETTRONICA ICAS mette a disposizione ai destinatari del presente Codice.

La sicurezza delle informazioni costituisce un valore imprescindibile per l'Azienda e per i suoi lavoratori, in particolare nell'ambito della postazione di lavoro, dei sistemi informatici aziendali e presso i cantieri dei clienti. Lo scopo del presente regolamento è quello di indicare i limiti entro cui i fruitori aziendali possono legittimamente usare le postazioni di lavoro ed i servizi Internet, evitando di esporre sé stessi e/o l'Azienda a gravi conseguenze che, in taluni casi, determinano ingenti sanzioni pecuniarie e, nei casi più gravi, possono investire il diritto penale.
Questo documento è stato implementato per tutelare la sicurezza dei Sistemi Informativi della EURELETTRONICA ICAS srl.

I Sistemi Informativi (hardware e software) e i dati aziendali in essi contenuti sono elementi essenziali per il successo della EURELETTRONICA ICAS srl. Essi sono, inoltre, parte del patrimonio EURELETTRONICA ICAS srl. In tal senso, tutte le risorse del sistema, inclusi l'attrezzatura, i programmi e tutti i dati inviati, ricevuti, salvati, e i mezzi di comunicazione resi disponibili sono e rimangono proprietà della EURELETTRONICA ICAS srl.
Ogni utente all'interno di EURELETTRONICA ICAS srl è responsabile nel proprio ambito della protezione delle informazioni e degli strumenti che in qualsiasi modo impiega durante lo svolgimento del proprio lavoro.
Ogni utente di EURELETTRONICA ICAS srl deve essere consapevole dell'importanza della sicurezza delle informazioni e deve operare in modo da garantire tale sicurezza.
In nessun caso l'utente dovrà utilizzare il Sistema Informativo aziendale per commettere un reato.
Per EURELETTRONICA ICAS garantire la sicurezza dei sistemi informativi significa:

- Assicurare la disponibilità delle risorse informative e dei dati.
- Assicurare l'integrità dei sistemi e dei dati.
- Assicurare la riservatezza delle informazioni.

3 DESTINATARI

Questo Codice di Condotta è valido per tutto il personale e per ogni altra persona autorizzata, anche in via temporanea, ad usare le attrezzature e i sistemi informatici e telematici della EURELETTRONICA ICAS srl. Queste persone verranno indicate nel seguito come "Utente" o come "dipendente".

4 RESPONSABILITÀ

- Ogni utente è responsabile dell'uso corretto delle risorse ICT
- E' vietato l'uso per fini personali non autorizzati, per attività illecite o per profitto privato
- E' d'obbligo di segnalare tempestivamente furti, danni o violazioni.

4.1 Responsabilità degli Utenti Individuali (A.5.2, A.5.4, A.5.11)

L'utente è autorizzato ad accedere alle risorse informative della EURELETTRONICA ICAS srl (inclusi hardware, software e dati, ma non solo) e accetta di essere pienamente responsabile per tutte le attività che svolge sul sistema informativo.
Resta inteso che tutte le risorse informative rimangono di proprietà della EURELETTRONICA ICAS srl e che l'Utente è consapevole e accetta di restituire la totalità delle risorse utilizzate nel momento in cui dovesse cessare il rapporto con EURELETTRONICA ICAS srl o nel caso in cui gli venisse richiesto dall'Azienda.

4.2 Uso professionale (A.5.10, A.5.32)

L'Utente accetta di usare i Sistemi Informativi per scopi professionali in relazione alla propria posizione all'interno della EURELETTRONICA ICAS srl. Le risorse relative ai Sistemi Informativi non verranno utilizzate per sviluppare o sfruttare programmi/dati a scopo personale o per terzi. In particolare, è proibito:

- Installare/utilizzare software non autorizzati dal Responsabile IT.
- Utilizzare i sistemi aziendali per servizi o comunicazioni illecite o illegali.
- Utilizzare le risorse aziendali per profitto personale.

I lavoratori dovranno quindi custodire diligentemente gli strumenti informatici e telematici ed i programmi, utilizzandoli solamente per fini professionali.

4.3 Protezione contro furti e danneggiamenti (A.7.3, A.7.8, A.7.9, A.7.13)

Per assicurare l'apparecchiatura dall'accesso non autorizzato, la stessa deve essere protetta portando a termine le sessioni attive e accertandosi che la password di protezione sia attivata quando l'apparecchiatura

viene lasciata incustodita (tranne, naturalmente, quando il computer deve rimanere aperto per un motivo specifico).
Tutta l'apparecchiatura portatile (computer portatili, tablet, etc.) deve essere custodita in luoghi chiusi a chiave o comunque in luoghi sicuri contro il furto. Quando essa è utilizzata fuori dell'edificio aziendale, devono essere prese tutte le precauzioni contro il furto non soltanto delle attrezzature, ma anche di tutti i dati riservati e/o importanti salvati sull'apparecchiatura.
L'Utente deve informare subito il Responsabile IT o l'AD di qualsiasi danno, furto o perdita di apparecchiatura, software e/o informazioni che gli sono state affidate.

4.4 Riservatezza e protezione del sistema e dei dati (A.5.15, A.5.12, A.5.13, A.5.33, A.5.34)

Nessun Utente può leggere o alterare le e-mail o le informazioni salvate su computer altrui, a meno che l'Utente non sia stato precedentemente autorizzato per iscritto dal Responsabile IT o AD.
L'Utente non è autorizzato ad accedere, né a tentare l'accesso, alle informazioni alle quali non ha normalmente privilegi di accesso. Se per errore, o a causa di un errato funzionamento del sistema, l'Utente ottenesse l'accesso a funzioni o informazioni normalmente non consentitegli, dovrà immediatamente chiudere il programma o il file nel quale è entrato e informare il Responsabile IT riguardo la situazione. È proibita ogni attività realizzata per violare, o per sollecitare la sicurezza del sistema, salvo autorizzazione esplicita scritta da parte del Responsabile IT.
Gli amministratori, utenti privilegiati che devono assicurare il corretto funzionamento e la sicurezza della rete e dei sistemi, sono obbligati a rispettare la totale riservatezza delle informazioni che incontrano. Di conseguenza, non possono utilizzare né divulgare le informazioni alle quali hanno accesso in veste di amministratori.
Si sottolinea che, in base alle normative sulla criminalità informatica, in caso di richiesta da parte dell'Autorità Giudiziaria, EURELETTRONICA ICAS srl metterà prontamente a sua disposizione tutte le informazioni in suo possesso della natura richiesta mantenendo, come previsto dalla legge, totale riservatezza verso terzi sia dell'avvenuta richiesta sia delle informazioni messe a disposizione.

4.5 Politiche di Clear desk e Clear Screen (A.7.7, 27018 A.11.7)

Al fine di ridurre il rischio di accesso non autorizzato ad informazioni aziendali, è necessario che l'utente segua delle politiche di clear desk e di clear screen. Con tali termini si intende che l'utente presti particolare attenzione a materiale cartaceo, dispositivi di memoria rimovibili e schermate a video contenenti informazioni non pubbliche. Di conseguenza, l'utente dovrà aver cura di distruggere o immagazzinare in luoghi sicuri stampe, memorie di massa portatili e simili. Particolare attenzione va posta alle stampe che, a volte, possono essere dimenticate sulle stampanti o ritirate dopo un tempo piuttosto lungo, lasciandole così incustodite e a disposizione di chiunque.
Anche le visualizzazioni a video possono contenere informazioni non pubbliche ed è quindi opportuno che tali schermate siano mantenute solo per il tempo strettamente necessario.
Anche l'utilizzo di riconoscitori vocali per la dettatura automatica deve seguire gli stessi principi.

- Protezione di documenti cartacei e schermate sensibili
- Distruzione sicura di stampe e supporti rimovibili

4.6 Integrità e disponibilità dei dati (cartelle di rete) (A.8.13, A.8.14, A.5.33)

L'integrità e la disponibilità dei dati aziendali è garantita dal Responsabile IT solo quando essi vengono trattati e memorizzati sul cloud, attraverso l'utilizzo delle "cartelle di rete" (*network folder*) assegnate a ciascun utente. L'utente è tenuto a trasferire tempestivamente e a mantenere nella propria cartella di rete i dati

considerati importanti o critici per la EURELETTRONICA ICAS srl o per la propria funzione specifica, eventualmente presenti localmente sul proprio PC. Resta pertanto inteso che eventuali dati memorizzati esclusivamente sulle postazioni di lavoro individuali non sono soggetti ad alcuna forma di protezione o salvataggio (backup) in caso di malfunzionamento, errore accidentale e/o manomissione.

4.7 Utilizzo strumenti informatici (A.5.10, A.8.19, A.8.18)

L'uso degli strumenti informatici è limitato alle necessità aziendali e professionali della EURELETTRONICA ICAS srl e deve avvenire secondo le disposizioni indicate nel presente codice.
Inoltre:

- È vietata l'installazione di software non autorizzato
- È obbligo un antivirus aggiornato
- E' obbligo seguire la Policy BYOD (Bring Your Own Device)

Policy BYOD – Bring Your Own Device

(A.6.7, A.7.9, A.8.1, 27018 A.11.5)

A. Scopo

Questa policy definisce le regole per l'utilizzo di dispositivi personali (smartphone, tablet, laptop) da parte dei dipendenti e collaboratori per accedere a risorse aziendali, garantendo sicurezza, conformità normativa e protezione dei dati.

B. Ambito di applicazione

La policy si applica a tutti i dipendenti, collaboratori e consulenti che utilizzano dispositivi personali per accedere a:

- *Email aziendale*
- *Rete interna*
- *Applicazioni e dati aziendali*
- *Piattaforme cloud e strumenti di lavoro*

C. Requisiti minimi dei dispositivi

I dispositivi personali devono:

- *Essere aggiornati con l'ultima versione del sistema operativo*
- *Avere software antivirus attivo e aggiornato*
- *Supportare l'autenticazione a due fattori (2FA)*
- *Essere protetti da PIN, password o biometria*

D. Sicurezza e protezione dei dati

- *È vietato memorizzare dati aziendali sensibili su dispositivi non cifrati*
- *I dati aziendali devono essere accessibili solo tramite app o ambienti autorizzati*
- *In caso di furto o smarrimento, l'utente deve informare immediatamente il Responsabile IT*
- *L'azienda si riserva il diritto di applicare soluzioni MDM (Mobile Device Management) per proteggere i dati*

E. Accesso e utilizzo

- *L'accesso alle risorse aziendali è consentito solo tramite VPN o connessioni sicure*
- *È vietato condividere credenziali aziendali con terzi*
- *L'uso del dispositivo deve rispettare le policy aziendali su privacy, sicurezza e comportamento*

F. Privacy dell'utente

- *L'azienda non accede ai dati personali (foto, messaggi, app private) del dispositivo*
- *Le attività aziendali possono essere monitorate solo nei limiti previsti dalla legge*
- *Ogni intervento tecnico sarà comunicato e documentato*

G. Responsabilità

- *L'utente è responsabile della sicurezza del proprio dispositivo*
- *L'azienda non è responsabile per danni, malfunzionamenti o perdita di dati personali*
- *L'utente accetta di rispettare tutte le disposizioni contenute nella presente policy*

H. Sanzioni

La violazione della policy può comportare:

- *Revoca dell'accesso alle risorse aziendali*
- *Provvedimenti disciplinari*
- *Segnalazione alle autorità competenti in caso di violazioni gravi*

I. Accettazione

Ogni utente che intende utilizzare un dispositivo personale per scopi aziendali deve:

- *Firmare il modulo di accettazione della policy BYOD*
- *Partecipare a una sessione di formazione sulla sicurezza informatica.*

4.8 Credenziali di accesso (A.5.16, A.5.17, A.8.5)

L'identità dell'utente è verificata attraverso lo "user-id" e la password a lui/lei assegnati, e tutte le attività svolte da un determinato user-id saranno attribuite al relativo utente. Pertanto, è di fondamentale importanza, ai fini della propria responsabilità, che l'utente tuteli le proprie credenziali ed in particolare la password contro l'indebita divulgazione. A tal fine sono state stabilite le seguenti misure di sicurezza:

- La password deve essere composta da almeno 8 caratteri e non sarà possibile inserire le ultime 10 password precedentemente utilizzate.
- La password non deve essere "banale", ossia non deve contenere alcun riferimento diretto a dati anagrafici e/o personali noti dell'utente (nome, cognome, data di nascita, matricola, ecc.).
- Ha una durata massima di 90 giorni.

Per un ulteriore livello di protezione, l'utente deve inserire nei caratteri della password lettere maiuscole, minuscole e/o numeri (es. Pass9Word). Deve pertanto:

- Memorizzarla.
- Non comunicarla mai ad altri
- Non trascriverla.
- Modificarla immediatamente in caso di sospetta violazione della sua segretezza.

Inoltre, al fine di evitare accessi indesiderati alla rete, anche durante piccole assenze dal posto di lavoro, è doveroso attivare uno screen saver con blocco della postazione, dotato di password, entro 5 minuti.
In sintesi:

- Obbligo di protezione delle credenziali.
- Introduzione dell'autenticazione a due fattori (2FA).
- Password robuste, rinnovabili ogni 90 giorni, non banali.

4.9 Personal Computer/portatile (A.7.8, A.7.9, A.8.1, A.8.23, A.8.24)

L'uso del personal computer/portatile è consentito esclusivamente per scopi aziendali.
Non è consentito installare, eseguire e/o scaricare qualunque tipo di software senza una preventiva autorizzazione scritta dal Responsabile IT.
Non è consentito riprodurre, tradurre, adattare, trasformare, distribuire software in licenza d'uso aziendale.
È assolutamente vietato memorizzare, utilizzare e/o installare strumenti hardware o software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici (a titolo esemplificativo: programmi di recovery password, cracking, sniffing, spoofing, serial codes, etc).
Non è consentito modificare autonomamente le configurazioni impostate sul proprio PC, né installare sullo stesso mezzi di comunicazione propri (ad esempio modem).
Non è consentito trasmettere, ricevere, scaricare, stampare o diffondere in qualunque altro modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale.
La password e gli strumenti di identificazione/autenticazione (smart card, badge, etc.) sono strettamente personali e non devono mai, per nessun motivo, essere ceduti o comunicati a terzi.
La gestione delle password deve essere conforme alle leggi vigenti in materia di protezione dei dati personali (cfr GDPR 2016/679).
Qualora l'utente abbia il ragionevole dubbio che le proprie credenziali di accesso siano state violate o abbia smarrito o gli sia stato rubato il dispositivo preposto per la memorizzazione delle stesse, egli ha l'obbligo di segnalare immediatamente l'accaduto al Responsabile IT.

Ogni personal computer/portatile deve avere installato il software antivirus standard aziendale, correttamente configurato ed aggiornato; è vietato disabilitare o inibire il corretto funzionamento del software antivirus.
Non è consentito condividere in rete file, stampanti, cartelle e altre risorse, salvo espressa autorizzazione da parte del Responsabile IT.
Ogni computer alla fine della giornata lavorativa deve essere spento o quanto meno le sessioni di lavoro devono essere chiuse (log-off). Potranno restare accesi solo computer per cui sia stata ottenuta una esplicita autorizzazione da parte del Responsabile IT.
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 (es. "blocca computer" tramite pressione contemporanea dei tasti Ctrl+Alt+Canc o la pressione del tasto logo Windows + L).
Non è consentito l'uso di dispositivi di memoria removibili.

4.10 Internet (A.5.14, A.8.20, A.8.21, A.8.22, A.8.23)

Internet è uno strumento messo a disposizione dell'Utente per uso professionale (eccezioni indicate nel §4.12-Uso personale). L'Utente deve quindi usare Internet in maniera appropriata tenendo presente che: (A.5.14, A.8.20, A.8.21, A.8.22, A.8.23)

- L'accesso ad Internet è assegnato individualmente all'Utente per permettergli di visitare per uso professionale, sotto il nome di "EURELETTRONICA ICAS srl", i siti disponibili in tutto il mondo. Tuttavia, è necessario considerare che quando si naviga nel Web l'identificazione dell'Utente, che compare sotto il nome di EURELETTRONICA ICAS srl sui siti esterni, ed i siti visitati vengono registrati entro i limiti della legge.
- Inoltre, ogni sito Internet può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.
- Tutte le azioni dell'Utente e tutti i dati riguardo all'Utente (siti visitati, messaggi scambiati, informazioni fornite tramite formati, dati raccolti all'insaputa dell'Utente, ecc.) possono essere registrati da chiunque all'esterno dell'Azienda ed analizzati per determinare i suoi interessi, gli interessi dell'Azienda ed usati per comunicati commerciali o per qualsiasi altro mezzo. L'Utente a tale riguardo deve prendere tutte le precauzioni necessarie.

A scopo di statistiche, qualità del servizio e sicurezza, il traffico Internet può essere controllato e possono essere fatte dalla EURELETTRONICA ICAS srl delle verifiche periodiche, entro i limiti legali.
L'uso di Internet è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate.
Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal proprio responsabile gerarchico e con il rispetto delle normali procedure aziendali di acquisto.
Non è consentito scaricare software gratuiti (freeware e shareware) prelevati da siti Internet se non espressamente autorizzati dal Responsabile IT.
È vietata ogni forma di registrazione con dati identificativi aziendali (es.: e-mail @eurelettronicaicas.com, numero telefonico aziendale, indirizzo aziendale ecc.) se non esplicitamente autorizzati dal proprio Responsabile.
È vietata comunque ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
Non sono permesse, per motivi non professionali, la partecipazione a forum, l'utilizzo di chat line, di bacheche elettroniche, social network e simili, anche utilizzando pseudonimi (o nicknames).
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.

Tutti i file di provenienza incerta o esterna, anche se 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 inoltrate al Responsabile IT.
Non è consentito l'invio di mail massive, ossia dirette ad un numero elevato di destinatari e con allegati di dimensioni significative, se non esplicitamente autorizzati dal Responsabile dei Sistemi Informativi e solo per scopi lavorativi, nel rispetto delle politiche e delle norme sul trattamento dei dati personali.
Non è consentito connettere, neanche per breve tempo, gli strumenti informatici aziendali (personal computer, portatili, ecc.) a reti esterne pubbliche (Internet), private (sistemi di altre società) o reti domestiche per mezzo di collegamenti fisici con linee telefoniche, PSTN, ISDN, xDSL o con strumenti wireless di qualsiasi genere. Da tale divieto sono da escludere gli accessi autorizzati dai clienti via VPN.
Non è consentito l'utilizzo di connessioni wi-fi di qualsivoglia natura senza l'utilizzo di opportune precauzioni (token o cifratura).
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 l'utilizzo della connessione ad Internet e, più in generale, delle connessioni di rete disponibili, per tentare accessi a sistemi su cui non si è autorizzati.
È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva della EURELETTRONICA ICAS srl o che possa essere nocivo all'immagine di EURELETTRONICA ICAS srl. Quindi, è proibita qualsiasi attività (di trasmissione / download / salvataggio / connessione) che può essere considerata come illegale, fraudolenta, spiacevole, di disturbo, offensiva, discriminatoria, diffamatoria, inclusa la connessione a siti pornografici o osceni.
Allo scopo di tutelare i propri sistemi informatici, la EURELETTRONICA ICAS srl adotta misure di protezione del traffico Internet anche mediante sistemi (surf control, firewall ecc.) finalizzati al blocco dell'accesso a determinati siti o contenuti. E' vietato aggirare o tentare di aggirare tali controlli (ad esempio mediante proxy anonimi).
In sintesi:

- Uso consentito solo per scopi professionali.
- Navigazione e comunicazioni monitorate nel rispetto del GDPR.
- Vietato l'uso di social network, forum e mailing list non autorizzati.
- Consentito l'uso moderato per fini personali, con separazione dei dati.

4.11 E-mail (A.5.14, A.5.33, A.5.34)

L'Utente non deve mai scrivere una e-mail il cui contenuto non possa essere espresso, convenientemente, oralmente né comunicato attraverso qualsiasi altro mezzo (messaggi digitali, ecc.), poiché la posta elettronica può essere:

- Salvata, riutilizzata o usata per fini che l'Utente può non aver considerato quando l'ha scritta.
- Usata come prova o come principio di prova scritta.

Inoltre, come anche in tutta la corrispondenza di affari, per tutti gli scambi di posta elettronica la cortesia è la regola basilare.
Deve essere sottolineato che un messaggio trasmesso tramite Internet può essere intercettato, anche illegalmente, letto, registrato ed utilizzato per altri fini da chiunque. Di conseguenza, nessuna informazione riservata dovrebbe essere trasmessa attraverso questo sistema, a meno che venga trasmessa attraverso una forma cifrata autorizzata (si veda §4.18-Limitazione all'utilizzo di sistemi di crittografia).
Non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate.

La classificazione di un messaggio e-mail come "confidenziale", "privato" o "personale", non sottrae il medesimo alla possibilità eventuale di una completa e totale verifica aziendale sull'attinenza del messaggio stesso all'attività lavorativa secondo le regole di incremento graduale del controllo esposte nel seguito.
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.
Le comunicazioni di maggior importanza e/o che contengano impegni per l'azienda devono essere sempre preventivamente autorizzate dal responsabile gerarchico competente.
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. Di conseguenza la partecipazione a forum di discussione e di "chat" è proibito se non autorizzato e attinente all'attività lavorativa.
Non è 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.
La posta elettronica non deve essere utilizzata per ricevere, memorizzare o spedire materiale che viola il copyright, il marchio o altre leggi sul diritto d'autore (cfr. ad esempio Leggi sul diritto d'autore D.Lgs. 68/2003).
Per limitare il fenomeno dello spamming è necessario 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
È proibito scaricare video, brani musicali ecc. e trasmettere e-mail a livello mondiale riguardanti argomenti personali.
È necessario fare attenzione alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti e devono essere notificati al Responsabile IT per la verifica.
Il tono, la presentazione e lo stile della posta elettronica devono riflettere l'immagine aziendale.
L'Utente non deve comunicare informazioni relative a EURELETTRONICA ICAS srl su Internet, se non previa approvazione dei responsabili.
Ogni e-mail inviata dovrà contenere, in calce, il disclaimer aziendale previsto.

4.12 Uso personale (A.5.10)

L'uso, esclusivamente occasionale e fortuito, di Internet e della posta elettronica per scopo personale sarà tollerato solo se questo non avrà un effetto negativo sul livello della performance dei sistemi o sull'attività lavorativa individuale e generale.
La EURELETTRONICA ICAS srl tollera un uso moderato per fini personali delle risorse tecnologiche messe a disposizione; l'Utente è responsabile, comunque, di registrare e conservare eventuali file contenenti propri dati personali, incluse le comunicazioni di posta elettronica, in un'apposita apposita cartella presente sul desktop del computer, denominata "Dati Personali", chiaramente individuata e protetta da password d'accesso gestita direttamente dall'Utente. Resta inteso che la manutenzione di tali file e cartelle, inclusi gli eventuali backup e restore è di esclusiva responsabilità dell'Utente, il quale manleva sin d'ora la EURELETTRONICA ICAS srl da ogni responsabilità in caso di distruzione o perdita degli stessi dati conseguenti ad un malfunzionamento, guasto od errore del sistema informatico, locale o centrale, sul quale tali dati siano registrati.
Qualora un assegnatario sia assente ed impossibilitato a recarsi in ufficio e EURELETTRONICA ICAS srl abbia l'esigenza di accedere al personal computer o all'utenza individuale, il Responsabile IT potrà richiedere per iscritto all'assegnatario di individuare un proprio "fiduciario", scelto a discrezione dell'assegnatario tra i dipendenti della EURELETTRONICA ICAS srl, al quale e solo al quale comunicare la propria password d'accesso. Al ritorno in servizio, l'assegnatario provvederà a cambiare la propria password.
Nel caso in cui non sia possibile comunicare con l'assegnatario, o questi non designi un proprio fiduciario, il Responsabile IT proverà. di "forzare" l'utenza impostando una nuova password che dovrà essere comunicata alla persona incaricata di effettuare l'accesso. Al primo ingresso con tali credenziali, il "fiduciario" dovrà immediatamente sostituire la password con una diversa solo a lui nota.

Al ritorno dell'assegnatario, il Responsabile IT provvederà ad effettuare una nuova "forzatura" impostando una nuova password per l'assegnatario che riprenderà ad operare normalmente, che potrà iniziare ad operare solo previa sostituzione della password con una diversa solo a lui nota.
Nel corso di queste operazioni non potranno essere oggetto di accesso i contenuti della cartella designata come contenente dati personali dall'assegnatario. A tale cartella, oltre al legittimo proprietario, potrà accedere solo l'Autorità Giudiziaria previo intervento di sblocco della password da parte dell'Amministratore di Sistema.

4.13 Uso condiviso (A.5.15)

L'utilizzo, da parte di colleghi o altri, dei sistemi informatici assegnati all'utente deve essere sorvegliato dall'utente stesso in quanto responsabile di garantire che tali sistemi non vengano utilizzati in violazione delle politiche di EURELETTRONICA ICAS srl o per compiere attività illegali.

4.14 End user computing (A.8.26, A.8.13, A.8.33)

Di norma le applicazioni utilizzate dovrebbero essere fornite dal Responsabile IT. In alcuni casi, per valide ragioni, l'utente (o addirittura un gruppo di utenti) potrebbe avere basato le proprie necessità elaborative anche su strumenti "sviluppati localmente". Tali strumenti possono essere, ad esempio, personalizzazioni fatte su strumenti di office automation quali fogli Excel, database Access o, addirittura, applicativi autorizzati e gestiti a livello della propria area. Nel seguito essi saranno definiti come end-user computing o, più brevemente EUC.
Tutte le tipologie di elaborazione appena descritte, trattando informazioni, devono essere gestite in maniera da garantirne la confidenzialità, l'integrità e la disponibilità. E' quindi essenziale che l'utente comunichi per tempo al proprio Responsabile l'esistenza di EUC di particolare criticità in modo che questi possa attivarsi per garantire almeno i seguenti requisiti:

- Esistenza di sufficiente documentazione
- Garanzia di backup e della possibilità di ripristino (con garanzia di inclusione nei test di ripristino dei dati salvati)
- Valutazione dei rischi legati all'utilizzo di EUC
- Controllo dell'ownership dell'EUC (ossia di chi è la responsabilità dell'EUC)
- Controllo dell'utilizzo, dei rilasci e di eventuali vincoli

4.15 Cloud e backup (A.5.23, A.8.13, 27018 A.11.3)

- I dati aziendali devono essere salvati su cartelle di rete o cloud aziendali.
- Backup automatici e protezione da perdita dati.

4.16 Controlli e monitoraggio delle risorse (A.8.15, A.8.16, A.8.17, 27017 A.12.4.5)

La EURELETTRONICA ICAS srl periodicamente o casualmente procederà, richiamate le garanzie della "privacy" previste dal GDPR 2016/679, anche ad un controllo quantitativo dell'utilizzo della rete, dei PC e della posta elettronica per verificarne un uso equilibrato e coerente con l'attività aziendale.
In particolare, a titolo esemplificativo, controlli periodici potranno essere effettuati su:

- Il volume dei messaggi scambiati
- Il formato dei file allegati
- La durata dei collegamenti ad Internet
- I siti visitati più frequentemente
- Le informazioni raccolte dai dispositivi di sicurezza (Firewall, Antivirus, IDS, ecc.)

Tali controlli avverranno secondo il principio dell'incremento graduale del controllo. In base a tale approccio, i controlli vengono svolti, inizialmente, su base aggregata e anonima. Nel caso venissero riscontrati parametri

anomali si potrà procedere all'individuazione delle Aree interessate da tali anomalie ed effettuare comunicazioni specifiche a tale livello. Se tali comunicazioni non dovessero portare ad una normalizzazione dei parametri misurati si potrà scendere, previo adeguato preavviso, a livello anche di singolo utente che, ove possibile, verrà invitato a partecipare direttamente alle attività di verifica.
Il monitoraggio non è finalizzato al controllo delle attività degli utenti (salvo eventuale esplicita richiesta in tal senso da parte delle Autorità competenti) ma solo al controllo dell'efficienza e dell'utilizzo corretto delle risorse informatiche aziendali e del network e si basa sul principio dell'incremento graduale del controllo stesso e, in generale, sul concetto di controllo difensivo ai sensi della legge.
I dati sopra descritti sono archiviati solo entro i limiti previsti dalla legge, salvo eventuale esplicita richiesta delle Autorità competenti.
In caso di attività sospette di gravità significativa queste potranno far scattare meccanismi di segnalazione all'Autorità Giudiziaria affinché avvii le indagini necessarie al fine di prevenire o sanzionare un reato, nell'ottica di tutelare gli interessi della EURELETTRONICA ICAS srl e dei suoi Clienti e Fornitori.
In conclusione: la EURELETTRONICA ICAS srl si riserva il diritto di controllare con apposite attività ispettive il rispetto delle norme indicate nel presente documento. Tali controlli saranno effettuati nella più stretta aderenza alle norme poste a salvaguardia della privacy dei dipendenti. Tali attività saranno svolte per quanto possibile esaminando le registrazioni informatiche di sintesi, senza esame dei contenuti delle registrazioni e della posta elettronica, salvo quanto previsto precedentemente. In ogni caso, ove siano necessari controlli che richiedano l'esame di contenuti, essi saranno condotti alla presenza dell'interessato, che potrà comunque impedire l'accesso ad informazioni da lui definite personali.
La Società si riserva inoltre il diritto di procedere ai controlli difensivi, previsti dalla legge e comunque di mettere in atto tutto le misure per assicurare la gradualità dei controlli.
In sintesi:

- I controlli ICT devono rispettare i principi di trasparenza, minimizzazione e finalità.
- Ogni attività di monitoraggio sarà documentata e comunicata agli utenti.

4.17 Software (A.8.19, A.8.18, A.5.32)

La ricezione e l'installazione di software può essere effettuata soltanto se viene precedentemente fornita un'approvazione scritta dalle persone autorizzate del Responsabile IT. L'Utente deve aderire a tutte le licenze dei software e copyright. Ciò include il divieto di copiare il software e installarlo su una postazione di lavoro diversa da quella autorizzata dal Responsabile IT.
La EURELETTRONICA ICAS srl richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'utente è tenuto ad osservare per un corretto utilizzo del software in azienda.
L'Azienda acquista le licenze d'uso del software per i computer da varie Società esterne. L'Azienda è soggetta a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e, a meno di una specifica autorizzazione concessa dallo sviluppatore del software, non ha il diritto di riprodurlo, salvo che per motivi di backup.
Per quel che riguarda le applicazioni in rete, i dipendenti dell'Azienda sono tenuti a utilizzare il software solo entro i limiti specificati nei contratti di licenza.
I dipendenti dell'Azienda non possono fare né il download né l'upload di software non autorizzato tramite Internet o tramite altri meccanismi.
Gli utenti che venissero a conoscenza di qualunque uso improprio del software o della relativa documentazione devono informarne immediatamente la funzione competente o l'ufficio legale dell'Azienda.
Secondo la legge sul copyright, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che 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.
Eventuali situazioni in cui un dipendente non sa se può copiare o utilizzare un determinato software devono essere discusse con un responsabile prima di procedere, ottenendone eventuale autorizzazione scritta. L'utente è consapevole della normativa che regola l'uso del software nell'Azienda e si impegna a rispettarla senza riserve.

4.18 Limitazione all'utilizzo di sistemi di crittografia (A.8.24)

È proibito cifrare le informazioni, nonché trasmettere, salvare o ricevere informazioni cifrate a meno che si ottenga precedentemente un'autorizzazione specifica dal Responsabile Sistemi Informativi della EURELETTRONICA ICAS srl.

5 VIOLAZIONE (A.6.4, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28)

La violazione da parte dell'Utente delle regole e degli obblighi esposti in questa linea guida porterà ad una appropriata azione disciplinare secondo quanto descritto nel Codice Disciplinare della EURELETTRONICA ICAS srl, azione che dipenderà dalla gravità dell'infrazione.
L'azione disciplinare intrapresa può variare dall'avvertimento scritto sino al licenziamento per grave inadempienza.
Per qualsiasi eventuale conseguente perdita finanziaria subita da EURELETTRONICA ICAS srl potrà essere fatta in tribunale una richiesta formale di risarcimento per danni. Inoltre, EURELETTRONICA ICAS srl informerà immediatamente le autorità esterne competenti nel caso che un qualsiasi reato venga commesso dall'Utente tramite il suo accesso ad Internet e/o ai Sistemi Informativi in generale.

6 FORMAZIONE E CONSAPEVOLEZZA (A.6.3, A.5.36)

Eurelettronica ICAS s'impegna nelle attività di formazione e consapevolezza degli aspetti legati alla sicurezza dell'informazione facendo in modo:

- Obbligo di partecipazione a corsi periodici sulla sicurezza informatica da parte del personale
- Diffusione di linee guida e aggiornamenti normativi a cura del Responsabile IT.

7 SEZIONE NUOVA – Segregazione dei compiti (A.5.3)

Per ridurre il rischio di errore o abuso, le attività che impattano la sicurezza sono soggette al principio di separazione tra chi richiede/approva e chi esegue. Le operazioni critiche, quali assegnazioni di privilegi amministrativi o modifiche a regole di sicurezza, richiedono doppia validazione. Gli account amministrativi sono separati da quelli di uso quotidiano e le operazioni sono tracciate in modo univoco.

8 SEZIONE NUOVA – Contatti con Autorità e gruppi di interesse; Threat Intelligence (A.5.5, A.5.6, A.5.7)

Il Responsabile IT mantiene i contatti con le Autorità competenti e con gruppi di interesse; il team IT rivede periodicamente le informazioni sulle minacce, emettendo quando necessario avvisi interni e coordinando attività di hardening o interventi straordinari.

9 SEZIONE NUOVA – Inventario degli asset (A.5.9)

L'azienda mantiene un inventario centralizzato degli asset informatici (modello EAD); per ogni elemento sono riportati almeno categoria, modello, numero di serie, proprietario. L'inventario è aggiornato a ogni consegna o rientro di asset.

10 SEZIONE NUOVA – Verifica indipendente della sicurezza e conformità (A.5.35, A.5.36)

Almeno annualmente la Direzione programma una verifica indipendente della conformità al Codice ICT e alle politiche di sicurezza. Le non conformità generano azioni correttive e aggiornamento della documentazione.

11 SEZIONE NUOVA – Uso della crittografia (A.8.24)

La crittografia viene adottata per proteggere i dati in transito e a riposo: i dispositivi portatili sono cifrati; le comunicazioni utilizzano protocolli sicuri; i documenti ed e-mail con contenuto Confidenziale sfruttano gli strumenti di Microsoft 365 per la protezione e la crittografia. La gestione delle chiavi segue le impostazioni del tenant; eventuali eccezioni sono motivate e approvate dal Responsabile ICT.

12 SEZIONE NUOVA – Classificazione ed etichettatura delle informazioni (A.5.12, A.5.13)

Le informazioni sono classificate in base alla loro archiviazione. Elementi non riservati vengono archiviati nelle cartelle "Commerciale/0 ESIS". Elementi riservati vengono archiviati nelle cartelle "ARAL".

13 APPENDICE A – Gestione degli incidenti di sicurezza

Il processo di gestione degli incidenti garantisce risposta tempestiva, riduzione dell'impatto e ripristino controllato dei servizi e dei dati. Ogni anomalia viene segnalata tempestivamente tramite i canali ufficiali; Il responsabile IT valuta la gravità e coordina gli interventi. Quando l'anomalia presenta impatti o rischi significativi per riservatezza, integrità o disponibilità, è qualificata come incidente e si attuano azioni ordinate: contenimento per limitare la propagazione, eradicazione della causa radice e ripristino. La comunicazione con gli stakeholder è proporzionata; se coinvolti dati personali, il referente privacy supporta valutazioni e adempimenti. Tutte le azioni sono documentate in un registro dedicato; al termine si svolge un'analisi delle lezioni apprese per pianificare gli interventi correttivi.

14 APPENDICE B – Ciclo di vita delle utenze e riesami degli accessi

Le identità e i privilegi seguono un ciclo di vita strutturato: all'ingresso si attiva un'utenza nominativa con MFA e si assegnano autorizzazioni per ruolo; nei cambi mansione le autorizzazioni sono adeguate e i privilegi non più necessari sono revocati; alla cessazione, account e accessi sono disabilitati nella stessa giornata, con rientro asset. Con cadenza trimestrale i proprietari dei dati verificano gli accessi alle aree informative, alle mailbox e ai gruppi, confermando o correggendo le autorizzazioni. Gli account amministrativi sono separati da quelli d'uso quotidiano e non sono ammessi account condivisi; le evidenze delle decisioni sono archiviate.

15 APPENDICE C – Data Loss Prevention e supporti rimovibili

Per prevenire perdite o esfiltrazioni di dati, sono adottate politiche DLP nella piattaforma Microsoft 365 e regole per l'uso dei supporti portatili. Le politiche sono progettate, comunicate e introdotte gradualmente, quindi monitorate per ridurre i falsi positivi; gli eventi significativi sono trattati come incidenti. I supporti rimovibili sono consentiti soltanto se cifrati e preventivamente autorizzati; l'uso di supporti personali è vietato.

16 APPENDICE D – Fornitori e supply chain

La sicurezza è integrata in tutto il ciclo di vita dei fornitori: valutazione pre-contrattuale proporzionata al rischio, clausole su riservatezza, notifica incidenti e livelli di servizio, onboarding con definizione di referenti e canali, monitoraggio periodico per i fornitori critici e gestione ordinata della fase di uscita con restituzione/cancellazione dei dati.

17 APPENDICE E – Sicurezza fisica e dei locali

Gli accessi agli uffici sono controllati; i visitatori sono identificati e accompagnati; le aree sensibili sono protette da chiusure e misure organizzative. Sono adottate dotazioni antincendio e gruppi di continuità per i sistemi critici, con manutenzioni pianificate e tracciate. Il cablaggio è posato in modo da ridurre il rischio di manomissioni o danni accidentali; nei lavori in aree protette si opera con autorizzazioni e dispositivi adeguati e nel rispetto delle regole del sito.

18 APPENDICE F – Logging, monitoraggio e sincronizzazione oraria

I log degli accessi e delle attività rilevanti su Microsoft 365 e sugli endpoint, insieme ai log degli apparati di rete e VPN, sono raccolti e conservati per un periodo minimo definito e protetti contro manomissioni. Sono configurati avvisi per tentativi di accesso anomali, malware e condivisioni esterne non autorizzate; un report mensile documenta anomalie e azioni. Tutti i sistemi utilizzano server NTP.

19 APPENDICE G – Sicurezza e segregazione di rete

La configurazione di firewall e VPN segue il principio del blocco predefinito, con aperture motivate e approvate; la rete è segmentata in domini separati per uffici, ospiti e laboratorio e la rete ospiti è isolata. L'accesso a servizi esterni è filtrato in base a categorie di rischio e le modifiche alle configurazioni sono tracciate; si verifica la segregazione tra ambienti virtuali e servizi cloud quando applicabile.

20 APPENDICE H – Continuità ICT e prove di ripristino

Sono definiti obiettivi di ripristino e continuità per i servizi critici e adottate misure di backup e ridondanza coerenti. Con cadenza almeno trimestrale si eseguono prove di ripristino con registrazione della sorgente, dei tempi e dell'esito, includendo la verifica dell'integrità dei dati; le risultanze guidano azioni correttive e il miglioramento dei piani.

21 APPENDICE I – Screening pre-assunzione e cambi ruolo

Per i ruoli con accesso a informazioni Confidenziali sono previsti controlli proporzionati prima dell'abilitazione ai sistemi; la risorsa sottoscrive gli impegni di riservatezza e prende visione del Codice ICT. In caso di cambio ruolo, il manager valuta la compatibilità dei privilegi e attiva gli adeguamenti necessari, assicurando che i permessi non più necessari siano revocati tempestivamente.

22 APPENDICE L – Change management, dati di test e audit-testing

Le modifiche significative seguono un processo autorizzato che definisce scopo, impatti, rischi e modalità di rollback; al termine è prevista una revisione dei risultati. I dati di test non utilizzano informazioni personali reali salvo anonimizzazione o mascheramento adeguato; al termine i dataset sono rimossi. Le attività di test di sicurezza sono pianificate con regole d'ingaggio chiare e i rilievi sono gestiti nel registro delle azioni correttive.

Per accettazione

Nome e cognome e firma del destinatario

_____