

Allegato 5.3
Descrizione delle misure
a contenimento del rischio di reato

Indice Misure

INTRODUZIONE

- 1. CONTROLLI ESTERNI**
- 2. POTERI**
- 3. PROCESSI DECISIONALI**
- 4. REGOLAMENTI E PROTOCOLLI RELATIVI ALL'EROGAZIONE DEI SERVIZI**
- 5. REGOLAMENTI E PROTOCOLLI RELATIVI ALLE ATTIVITÀ DI STAFF**
 - a) Procedure di acquisto**
 - b) Regolamento contabile**
 - c) Procedure per adempimenti fiscali**
 - d) Regolamento per sponsorizzazioni**
 - e) Procedura per la protocollazione e la conservazione della documentazione aziendale**
 - f) Procedura di selezione del personale dipendente**
 - g) Procedura di selezione di un collaboratore o di un professionista**
 - h) Procedura relativa alla gestione degli adempimenti per l'instaurazione e gestione del rapporto di lavoro**
 - i) Norme di servizio per il personale dipendente di livello non dirigente;**
 - j) Procedura di rimborso spese viaggi**
 - k) Procedura carte di credito aziendali**
 - f) Regole per l'uso dei sistemi informatici e per la tutela del diritto d'autore e dei segni distintivi**
 - g) Procedura per il controllo periodico del software installato**
 - h) Procedura di gestione dei rifiuti**
- 6. MISURE DI SICUREZZA INFORMATICA**
- 7. MISURE DI PREVENZIONE E PROTEZIONE DELLA SICUREZZA E DELLA SALUTE DEI LAVORATORI**
- 8. VINCOLI CONTRATTUALI CHE IMPONGONO AGLI OUTSOURCER L'ADOZIONE DI MISURE A CONTENIMENTO DEL RISCHIO DI REATO**

INTRODUZIONE

A seguito dell'adozione del Piano di Prevenzione della Corruzione da parte di Camera Arbitrale, i protocolli e le procedure adottati dall'azienda a presidio dei rischi relativi ai reati elencati nel D.lgs 231/2001, varranno anche per i reati elencati nella legge 190/2012. Il rispetto dei protocolli e procedure a presidio dei reati di corruzione è di competenza sia del Responsabile di Prevenzione della Corruzione sia dell'Organismo di Vigilanza.

1) CONTROLLI ESTERNI

La revisione contabile è affidata al Collegio Sindacale nominato con delibera dal Consiglio di Amministrazione.

Il servizio di cassa è affidato per Statuto all'Istituto cassiere della Camera di Commercio di Milano.

2) POTERI (DA AGGIORNARE CON QUANTO PREVISTO IN STATUTO / POTERI SA)

Fonte	Poteri
Consiglio di amministrazione	
Statuto	E' investito dei più ampi poteri per la gestione ordinaria e straordinaria della società
	Approva i regolamenti e i tariffari per definire le modalità di svolgimento dei servizi di cui all'articolo 2 dello Statuto (arbitrato, conciliazione, mediazione, perizia contrattuale, arbitraggio ed altri)
	Delibera la nomina del Consiglio arbitrale
	Delibera, nelle forme e nei limiti di legge, la fusione e la scissione nelle ipotesi degli artt. 2505 e 2505 bis c.c., quale richiamato anche dall'art. 2506 ter c.c.
	Nomina il Direttore generale e i procuratori per il compimento di determinati atti
	Predisporre i piani di sviluppo della CAMERA ARBITRALE DI MILANO s.r.l., adotta i provvedimenti necessari per la loro realizzazione in conformità agli indirizzi stabiliti dagli organi della Camera di Commercio di Milano - Monza Brianza - Lodi e fissa i parametri di valutazione dell'efficacia e dell'efficienza dell'azione aziendale
	Nomina il Presidente ed il Vicepresidente
	Può nominare un Amministratore Delegato ovvero, previa autorizzazione dell'Assemblea, delegare le proprie funzioni al Presidente
	Procede alla formazione del bilancio da presentare ai soci entro 120 giorni dalla chiusura dell'esercizio sociale, ovvero entro centottanta giorni, quando lo richiedono particolari condizioni, nei limiti ed alle condizioni di cui all'art. 2364, secondo comma, c.c..
Presidente	
Statuto	Rappresentanza legale
	Convoca e presiede il Cda
	Presiede l'Assemblea dei soci
Direttore Generale	
Per Statuto	Capo del personale
	E' responsabile dell'esecuzione delle decisioni del CdA
	Provvede alla gestione degli affari correnti
	Sovrintende all'organizzazione ed al funzionamento della società
	Spetta, nei limiti delle attribuzioni conferite ,la rappresentanza legale della società di fronte ai terzi e in giudizio
In virtù del dpr 254/05	Sottoscrive i mandati di pagamento a firma congiunta con il Responsabile Amministrativo
Responsabile Amministrativo	
In virtù del dpr 254/05	Sottoscrive i mandati di pagamento a firma congiunta con il Direttore Generale

3) PROCESSI DECISIONALI

I processi decisionali, che coinvolgono più soggetti, stabiliti dallo Statuto, sono i seguenti:

Approvazione del preventivo economico e del bilancio	
CdA	Consiglio della CCIAA
D	A

Deliberazioni che vincolano il bilancio oltre l'anno	
CdA	Giunta della CCIAA
D	A

Deliberazione sul regolamento di organizzazione, e altri regolamenti	
Direttore Generale	CdA
PS	D

Deliberazione sulla pianta organica	
CdA	Giunta della CCIAA
PS	A

Deliberazione in ordine all'assunzione, trattamento economico, carriera e cessazione del rapporto di lavoro dei dirigenti e responsabili di divisione	
Direttore Generale	CdA
PS	D

Stanziamento complessivo per i premi al personale	
Direttore Generale	CdA
PS	D

Attribuzione dei premi ai dirigenti	
Direttore Generale	CdA
PS	D

Nomina del dirigente con funzioni vicarie del Direttore Generale	
Direttore Generale	CdA
PS	D

Approvazione delle tariffe dei servizi	
Direttore Generale	CdA
PS	D

A Approva D Decide PS Proposta

I processi decisionali aziendali disciplinati sono i seguenti:

- a. processo per l'adozione di determinate del Direttore Generale e del Presidente;
- b. processo per la gestione delle fatture passive;

- c. processo per la gestione dei mandati di pagamento e delle reversali di pagamento;
- d. processo per la gestione degli ordini di acquisto;
- e. processo per la gestione delle richieste di acquisto.

Processo per l'adozione di determine del Direttore Generale e del Presidente				
Addetto/Responsabile/ Dirigente Unità Organizzativa	Amministrazione CA	Responsabile Risorse	Direttore Generale	Presidente
E	C	C	A	A

Processo per la gestione delle fatture passive			
Segreteria Arbitrato o Mediazione	Funzionario/ addetto	Direzione Generale	Amministrazione
E, C	E, C	E	A

Processo per la gestione dei mandati di pagamento e delle reversali di pagamento		
Segreteria Arbitrato o Mediazione	Contabilità e Bilancio AS	Direttore Generale o suo delegato
E	C	A

Processo per la gestione degli ordini di acquisto					
Responsabile dell'iniziativa	Amministrazione	Responsabile Contabilità e Bilancio	Ufficio Acquisti	Direttore Generale	Direzione Generale
E	C	C	E	A	E

Processo per la gestione delle richieste di acquisto		
Addetto Unità Organizzativa	Direttore Generale	Ufficio Acquisti
E	A	E

E Esegue C Controlla A Autorizza

4) REGOLAMENTI E PROTOCOLLI RELATIVI ALL'EROGAZIONE DEI SERVIZI

Il servizio di arbitrato è disciplinato dal Regolamento Arbitrale che descrive:

- la fase iniziale, con la domanda di arbitrato;
- il tribunale arbitrale;
- il procedimento arbitrale;
- il lodo arbitrale;
- i costi del procedimento, con i criteri di determinazione del valore della controversia e gli onorari della Camera arbitrale, le tariffe;
- il codice deontologico dell'arbitro;
- il ruolo e la composizione del Consiglio arbitrale;
- il ruolo e la composizione della Segreteria Generale.

E' adottata una disposizione relativa all'uso dei valori bollati sugli atti relativi al procedimento arbitrale.

Il servizio di Conciliazione svolge alcuni servizi di mediazione disciplinati da specifico Regolamento:

- il Regolamento di mediazione che definisce anche l'indennità per il servizio di mediazione e il codice etico per i mediatori;
- il Regolamento dell'Italy China Business Mediation Center;
- il Regolamento per la risoluzione delle dispute nel country code Top Level Domain "it"
- il Regolamento per il servizio RisolviOnline.

Il servizio di Conciliazione svolge la propria attività seguendo uno specifico Vademecum. Regolamenti e Vademecum sono riportati all'allegato 1.

a) PROCEDURE DI ACQUISTO Le procedure di acquisto sono gestite dall'Ufficio Acquisti conformemente al Processo degli Acquisti di Camera Arbitrale (all. 2).

b) REGOLAMENTO CONTABILE

E' adottato un nuovo regolamento di contabilità.

c) PROCEDURE PER ADEMPIMENTI FISCALI (a contenimento reati fiscali)

Il Regolamento è riportato all'allegato 4

Dichiarazione Redditi	Le dichiarazioni (la dichiarazione dei redditi, IVA, Irap, Ires) sono predisposte dall'Ufficio Fiscalità della Camera di Commercio sulla base delle informazioni fornite da Contabilità e Bilancio AS (ritenute per i lavoratori autonomi) e dall'outsoucer esterno che produce i cedolini paga (ritenute per i dipendenti) L'Ufficio Fiscalità si avvale del supporto di uno studio commercialista esterno, che tra l'altro, provvede all'invio delle dichiarazioni La dichiarazione 770 è predisposta dall'outsourcer esterno che produce i cedolini paga. Le informazioni relativi alle ritenute per i lavoratori autonomi sono fornite da Contabilità e Bilancio AS. Lo stesso outsourcer provvede all'invio delle dichiarazioni.
Chiusure IVA e relativa liquidazione	
Liquidazione Ritenute d'acconto, certificazioni e riepiloghi fiscali	
Tenuta libro cespiti Tenuta libro IVA Tenuta libro Inventari	Competenza di Contabilità e Bilancio
Fatture	Si vedano procedure contabili

d) PROCEDURA OMAGGI E SPONSORIZZAZIONI

1. Omaggi

- a. I dipendenti e dirigenti di Camera Arbitrale non possono ricevere omaggi se non di modesto valore. Nel caso in cui siano destinatari di omaggi di valore non modesto ne informano per iscritto il Direttore Generale che deciderà in merito.
- b. I dipendenti e dirigenti di Camera Arbitrale non possono fare omaggi a terzi, qualunque essi siano, se non espressamente approvati dal Direttore Generale.
- c. Il Direttore Generale sceglie ogni anno gli omaggi natalizi, che debbono avere carattere simbolico e debbono essere di modesto valore. Sono esclusi altri omaggi, diversi da quelli natalizi, a meno che essi non siano giustificati da eventi eccezionali e da ragioni di cortesia. Anche in questo

caso gli omaggi dovranno avere carattere simbolico ed essere di modesto valore.

- d. Le spese per gli omaggi debbono essere contabilizzate come tali in modo da consentirne un'immediata identificazione

2. Inviti, viaggi, prestazioni varie

- a. I dipendenti e dirigenti di Camera Arbitrale non possono ricevere da terzi inviti a iniziative e/o viaggi e comunque prestazioni varie, a meno che non siano strettamente attinenti all'attività lavorativa e rientrino in eventi promozionali e di pubbliche relazioni. In questi casi, ne informano per iscritto il Direttore Generale che deciderà in merito.
- b. I dipendenti e dirigenti di Camera Arbitrale non possono offrire a terzi inviti a iniziative e/o viaggi e prestazioni varie a meno che non siano funzionali ad eventi di comunicazione e promozione di Camera Arbitrale ed attengano strettamente ad esse. In questi casi, tali iniziative debbono essere approvate dal Direttore Generale, secondo i propri limiti di spesa, o dal Consiglio di Amministrazione, che dispongono anche in merito alle modalità e ai limiti delle offerte.
- c. Le spese per tali prestazioni debbono essere contabilizzate come tali in modo da consentirne un'immediata identificazione. Devono essere indicati l'ambito dell'iniziativa e le persone a cui la prestazione è diretta.

3. Sponsorizzazioni

- a. Eventuali sponsorizzazioni di Camera Arbitrale ad iniziative, sia pubbliche che private, debbono essere autorizzate dal Direttore Generale, secondo i propri limiti di spesa, o dal CdA, sentito l'OdV.
- b. L'eventuale sponsorizzazione di iniziative private è subordinata all'applicazione della procedura di verifica dell'affidabilità del partner.
- c. Eventuali sponsorizzazioni da parte di soggetti pubblici e privati a favore di Camera Arbitrale debbono essere autorizzate dal Direttore Generale sentito l'OdV.
- d. L'eventuale sponsorizzazione da parte di soggetti privati è subordinata all'applicazione della procedura di verifica dell'affidabilità del partner. La Società ha adottato il Regolamento per le sponsorizzazioni a cui si rimanda per ulteriori disposizioni.

e) PROCEDURA PER LA PROTOCOLLAZIONE E LA CONSERVAZIONE DELLA DOCUMENTAZIONE AZIENDALE

A partire da settembre 2018 Camera Arbitrale ha adottato Gedoc, l'applicativo già in uso da parte della CCIAA di Milano Monza Brianza Lodi per la protocollazione e conservazione a norma dei documenti informatici.

g) PROCEDURA DI SELEZIONE DEL PERSONALE DIPENDENTE

Si rinvia al Regolamento interno per la selezione di personale dipendente

h) PROCEDURA DI SELEZIONE DI UN COLLABORATORE O DI UN PROFESSIONISTA

Si rinvia al Regolamento per il conferimento di incarichi ad esperti esterni a Camera Arbitrale srl.

i) PROCEDURA RELATIVA ALLA GESTIONE DEGLI ADEMPIMENTI PER L'INSTAURAZIONE E GESTIONE DEL RAPPORTO DI LAVORO

Gestione amministrazione del personale

Descrizione: - Gestione dei rapporti amministrativi del personale ed aggiornamento dei relativi libri obbligatori

Tutte le procedure di comunicazione agli Enti sono effettuate tramite accessi via Web personalizzati con chiavi di identificazione dei soggetti registrati

- **Comunicazioni Obbligatorie** (Decreto Interministeriale 30/10/2007) di assunzioni/dimissioni/modifica del rapporto di lavoro/proroga /trasformazione : procedura COB (unificata) attraverso il Portale della Provincia di Milano da parte di utente autorizzato e registrato, autenticato con PIN e password Azienda
- **INPS** adempimenti per iscrizione del lavoratore/flusso e-mens/ denunce DM10: procedura UNIEMENS accesso effettuato da utente autorizzato e registrato, autenticato con PIN e password
- **INAIL** – tenuta del Libro Unico del lavoro (LUL) sul quale sono iscritti i lavoratori subordinati, i collaboratori coordinati e continuativi, si dispone di autorizzazione, emessa preventivamente dall'INAIL alla stampa e alla generazione della numerazione automatica; adempimenti per denuncia infortunio, denuncia annuale contributiva per l'autoliquidazione del premio assicurativo, attraverso il portale da parte di utente registrato e autorizzato, autenticato con PIN e password.

Inoltre

- **QUAS** – Cassa assistenza sanitaria quadri del terziario – comunicazioni di assunzione e cessazione quadri, accesso attraverso il portale da parte di utente registrato e identificato con Pin e password
- Verifica del possesso del permesso di soggiorno per il personale extracomunitario.

Ulteriori adempimenti verso Fondi Pensionistici Complementari di categoria ovvero Fondi assicurativi c.d. aperti - accesso via Web ai singoli portali da parte di utente registrato con PIN e password.

j) NORME DI SERVIZIO PER IL PERSONALE DIPENDENTE DI LIVELLO NON DIRIGENTE

Sono fissate le norme a cui il personale deve attenersi nello svolgimento della propria attività lavorativa:

- orario di lavoro
- timbrature
- ritardo
- permessi retribuiti
- malattia
- ferie
- festività soppresse
- straordinario
- recuperi
- missioni
- buoni pasto
- comunicazioni di mutamento di domicilio/residenza

- sanzioni

k) PROCEDURA DI RIMBORSO SPESE VIAGGI

La procedura disciplina le modalità di rimborso spese. Qui rileva per i controlli delle spese effettuate.

Il modulo di nota spese, redatto dal dipendente, viene sottoposto alla firma del responsabile del dipendente a cui la nota si riferisce, che verifica l'osservanza della procedura, le percorrenze, le visite e tutto quanto sia giustificato da ragioni operative. La nota spese viene poi trasmessa al Dirigente superiore che la autorizza. Va quindi inoltrata all'Amministrazione che effettua controlli amministrativi e fiscali:

- i. controllo di tutte le somme;
- ii. controllo dell'esistenza di pezze giustificative;
- iii. controllo dell'esatta applicazione delle tariffe di rimborso;
- iv. controllo ammontare anticipi e biglietti viaggio.

	Dipendente	Dirigente	Responsabile del dipendente	Direttore Generale	Amministrazione
Nota spese del dipendente	Redige		Controlla l'osservanza della procedura, le percorrenze, le visite e tutto quanto giustificato da ragioni operative	Autorizza	Effettua controlli amministrativi e fiscali
Nota spese del dirigente		Redige		Autorizza	Effettua controlli amministrativi e fiscali

Le spese di rappresentanza/colazioni di lavoro devono essere di norma preventivamente approvate dal Direttore generale e sono rimborsabili purché sia chiaramente indicata la natura, l'importo e lo scopo delle spese, oltre al nome delle persone che ne hanno fruito, la posizione e società/studio legale/ente che rappresentano.

	Direttore Generale	Dipendente/Dirigente
Spese di rappresentanza	Approva preventivamente la spesa	Compila la nota spese indicando la natura, l'importo, lo scopo e la persona che ne ha fruito, indicando la sua posizione e la società che rappresenta

Nel caso di partecipazione retribuita ad eventi esterni (convegni, corsi di formazione etc.), il compenso deve essere versato alla Camera Arbitrale. Le spese di soggiorno e/o viaggio sono a carico della Camera Arbitrale e rimborsate secondo le disposizioni previste.

Si rinvia alla Procedura di Rimborso spese viaggi per ogni ulteriore previsione.

I) PROCEDURA CARTE DI CREDITO AZIENDALI

La procedura disciplina le modalità di rilascio e utilizzo della carta di credito aziendale. Qui rileva per i controlli delle spese effettuate, affidate all'Ufficio Amministrazione.

Le spese effettuate con carta di credito debbono risultare dalla nota spese che subisce il controllo previsto dalla Procedura Rimborso spese viaggi.

m) REGOLE PER L'USO DEI SISTEMI INFORMATICI E PER LA TUTELA DEL DIRITTO D'AUTORE E DEI SEGNI DISTINTIVI

1. Stazione di lavoro

La stazione di lavoro (pc, laptop, portatile etc.) affidata all'utente è uno strumento di lavoro. Deve essere custodita con cura evitando ogni possibile forma di danneggiamento.

2. Protezione della stazione di lavoro

L'utente deve mettere in atto tutte le precauzioni possibili al fine di evitare accessi indesiderati o non controllati alla propria dotazione di informatica individuale, in particolare deve:

- assicurarsi che la workstation assegnatagli sia dotata di password all'accensione, in caso contrario deve segnalarlo al proprio responsabile
- se durante l'orario di lavoro lascia incustodita la workstation, deve alternativamente:
 - spegnere la workstation
 - bloccarla
 - effettuare il logout della sessione utente
- attivare comunque, ovunque possibile, il salvaschermo (screen-saver automatico con password) entro i 10 minuti di inutilizzo
- al termine della giornata di lavoro spegnere la workstation oppure disconnettersi dalla propria sessione e passare alla modalità di stand-by o di risparmio energetico.

Nel caso in cui l'utente disponga di portatile, è tenuto a:

- proteggerlo con la password secondo le istruzioni fornite;
- non lasciarlo incustodito, specie in ambienti pubblici
- quando non serve, riporlo sotto chiave
- non registrarvi informazioni sensibili o riservate e, qualora non se ne possa fare a meno, crittografarle.

L'utente è responsabile di fornire il proprio contributo al fine di minimizzare la possibilità che i dati personali o riservati contenuti nella propria workstation o trattati tramite la workstation siano esposti a rischi di sicurezza.

3. Manutenzione di informazioni critiche su workstation

E' vietato conservare/mantenere esclusivamente sulla propria workstation, quale archivio o sorgente informativa primaria, archivi/database di dati critici per il business aziendale e/o classificabili come 'personali/sensibili/giudiziari', senza segnalarlo al proprio responsabile gerarchico, per le opportune contromisure, esponendoli quindi al rischio di perdita o danneggiamento anche involontario.

4. Dati personali del dipendente e dismissione delle apparecchiature

La registrazione di dati personali non aziendali da parte dei dipendenti su workstation è ammessa, nel rispetto delle politiche di sicurezza, a meno che non comprometta la

funzionalità della workstation e previa separazione (cartelle ad hoc facilmente distinguibili da quelle contenente dati aziendali) o cifratura di tali dati.

All'atto della dismissione, riassegnazione e qualora comunque necessario, è opportuno che anche il dipendente proceda alla *cancellazione sicura* dei propri dati personali eventualmente memorizzati sulla workstation in forma intellegibile.

5. Password e regole relative

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia degli asset aziendali e dell'utente stesso.

Le regole di seguito elencate sono vincolanti per l'accesso a tutti i sistemi e le workstation.

a. Impostazione, variazione iniziale e periodica delle password

- Le password assegnate per qualsiasi scopo devono essere sostituite al primo utilizzo.
- Tutte le password di default (ad es. “system”, “administrator”) devono essere cambiate al momento dell’installazione del prodotto o del sistema.
- Tutte le password devono essere cambiate almeno ogni 6 mesi a cura degli incaricati (titolari delle credenziali) ovvero ogni 3 mesi nel caso di accesso a dati sensibili ai sensi della normativa in materia di privacy

b. Regole di utilizzo generali

- Le password non devono essere scritte in chiaro
- Le password non devono essere inserite in chiaro in messaggi e-mail o in altre forme di comunicazione elettronica
- Le password non devono essere comunicate a terzi dal titolare.
- Nel caso in cui il titolare sospetti che la sua password sia venuta a conoscenza di terzi deve essere immediatamente cambiata
- E' obbligatorio custodire idoneamente smart-card, token e business-key contenenti certificati di autenticazione e disinserire i predetti dispositivi dal computer prima di lasciarlo incustodito

c. Gestione delle password nei sistemi

La password dell’utente non deve essere registrata in nessun modo nel log delle sessioni e neppure in nessun altro sistema di logging / debugging.

d. Caratteristiche obbligatorie delle password

La lunghezza minima della password è di 8 caratteri o comunque il massimo previsto dalla tecnologia o sistema specifico.

Inoltre la password :

- deve contenere almeno un carattere alfabetico ed uno numerico.
- non deve contenere più di due caratteri identici consecutivi.
- non deve essere simile alla password precedente.
- non deve contenere l’user-id come parte della password.
- non deve essere riconducibile ai dati anagrafici dell’incaricato o di suoi familiari

e. Suggerimenti per la costruzione di password robuste

Le password devono essere ricordabili facilmente ma devono essere al contempo robuste. Un modo per ottenere ciò è costruire password che si basino sul titolo di una canzone, su di una frase storica o su di una poesia e assemblarne i pezzi.

Ad esempio, la poesia potrebbe essere: “Mi illumino di immenso” ed una password ricavabile da quella poesia potrebbe essere costruita prendendo le prime due lettere di ogni parola con la prima in carattere maiuscolo ottenendo: “MiIlDiIm”.

Da “Quel mazzolin di fiori” si può ottenere: “QuMaDiFi”.

Per inserire anche caratteri numerici si può sostituire le “i” con il numero “1” o le “o” con lo zero.

Nel seguito sono descritte le caratteristiche delle password robuste e le caratteristiche delle password deboli.

- Password robuste

Una password intrinsecamente robusta ha le seguenti caratteristiche:

- Contiene sia caratteri maiuscoli sia caratteri minuscoli
- Contiene cifre, lettere maiuscole e minuscole e altri caratteri ammessi dal sistema in uso
- E' lunga più di otto caratteri
- Non è una parola di una qualunque lingua, dialetto o linguaggio specialistico
- Non si basa su informazioni personali

- Password deboli

Una password intrinsecamente debole ha una o più delle seguenti caratteristiche:

- è una parola che si trova sul vocabolario
- è una parola di uso comune come, ad esempio: nomi propri, cognomi, personaggi di fantasia (es. Mario, Rossi, Pluto, ...)
- è il nome dell'ente o dell'azienda
- è una data di nascita, un indirizzo, un numero di telefono, una targa automobilistica
- è una sequenza banale di caratteri come, ad esempio: aaabbb, qwerty, 123456
- è una qualsiasi password precedentemente menzionata scritta a rovescio
- è una qualsiasi password precedentemente menzionata preceduta o seguita da una cifra

L'aggiunta di cifre prima o dopo una password debole non modifica la sua debolezza (es. Mario99 o 99Mario sono password deboli).

f. Framework di supporto

Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.

g. Ripristino della password

Il ripristino della password deve essere eseguito mediante apposita procedura, solo a fronte di una positiva identificazione del richiedente.

La nuova password ottenuta dovrà essere cambiata subito dopo a cura del richiedente stesso.

6. Software

I software non correlati allo svolgimento della specifica attività lavorativa e al di fuori degli standard aziendali, non hanno a priori alcun titolo per essere presenti nelle stazioni di lavoro individuali.

La responsabilità relativa all'installazione dei predetti software è pertanto di chi li installa sulla stazione di lavoro, a meno di documentabile specifica autorizzazione aziendale.

L'installazione da parte del dipendente di software non previsto dalla dotazione standard aziendale sulla propria stazione di informatica individuale o non specificamente autorizzata è ammessa, a responsabilità del dipendente stesso, esclusivamente a condizione che tali software:

- siano compatibili con la funzionalità della stazione di lavoro e con l'espletamento delle mansioni lavorative del dipendente
- non siano pericolosi per la sicurezza delle informazioni aziendali
- non siano in contrasto con le normative di legge, con particolare attenzione a:
 - norme in materia di protezione dei dati personali;

- norme in tema di copyright;
- norme contro i reati informatici;
- politiche di sicurezza aziendali.

Il software che venga rilevato/segnalato in contrasto con quanto sopra detto, deve essere immediatamente rimosso a cura del dipendente stesso.

7. Tutela del software

I software debbono essere acquisiti con regolare licenza e devono essere conservate le prove della titolarità della licenza. E' quindi proibito installare software senza licenza. Per licenza si intende ogni tipo di atto che consente l'utilizzo del software quale, a titolo d'esempio: le licenze di tipo proprietario che consentono solo l'uso del software, le licenze freeware che ne consentono l'uso e la distribuzione, le licenze shareware che subordinano l'uso del software a determinate condizioni, le licenze del free-software o del software open source che ammettono anche l'accesso e la modifica del codice sorgente.

Considerando le varie tipologie di licenze e la conseguente diversa disciplina dei diritti sul software è necessario che quanto da esse disposto sia conosciuto e se ne dia scrupolosa attuazione.

L'utilizzo di software freeware e shareware è consentito solo nel caso in cui i programmi siano scaricati da fonti sicure. Sono fonti sicure quelle che danno garanzia che:

- la distribuzione del software avvenga nel rispetto dei relativi diritti;
- il software distribuito sia esente da codice malevolo (virus, network worms, trojan horses, logic bombs etc.)

L'utilizzo di free software o di software open source è consentito nei limiti e alle condizioni prescritte dalla relativa licenza, con riferimento in particolare ai vincoli previsti nel caso di distribuzione successiva dello stesso software o delle sue modifiche/integrazioni/evoluzioni.

Nel caso in cui lo sviluppo del software sia affidato a terzi, è necessario assicurarsi, anche contrattualmente, che il software eventualmente impiegato per lo sviluppo sia utilizzato legittimamente nel rispetto del diritto d'autore.

8. Tutela di altri materiali protetti dal diritto d'autore e/o dalla disciplina sui marchi e segni distintivi

L'utilizzo di brani, musica, video, fotografie o altro materiale protetto dal diritto d'autore per la realizzazione di filmati promozionali, presentazioni, report etc. è consentito solo con l'autorizzazione del titolare dei diritti e comunque a condizione di aver verificato il regime d'utilizzo di tali opere e averlo rispettato. A questo proposito si suggerisce di utilizzare materiale distribuito con licenza Creative Commons che non escluda l'utilizzo commerciale del materiale.

Salvo il caso di cui al punto precedente, è assolutamente vietato utilizzare gli strumenti aziendali per scaricare materiale protetto dal diritto d'autore.

L'utilizzo di segni distintivi altrui nell'ambito di iniziative congiunte è consentito solo previa autorizzazione scritta del titolare del segno. Senza il consenso del titolare, non è in alcun modo ammesso l'utilizzo di marchi, loghi e segni distintivi altrui per promuovere direttamente o indirettamente (ad esempio attraverso i metatag) le iniziative dell'azienda sul web.

9. Strumenti di controllo

Sono adottati adeguati strumenti di controllo ed effettuati audit interni, anche automatici, in modo tale da verificare che il software o altro materiale protetto dal diritto d'autore (quale video, musica, foto etc.) presente sui computer in dotazione possa essere lecitamente utilizzato. E' proibito inabilitare l'uso di tali strumenti di controllo.

10. Utilizzo corretto di Internet e Posta elettronica

L'azienda mette a disposizione dei dipendenti i servizi di posta elettronica e l'accesso alla rete internet. Nell'utilizzare tali strumenti il dipendente è tenuto ad operare secondo correttezza.

- L'utilizzo dei servizi di posta elettronica e di Internet è consentito:
 - solo attraverso le infrastrutture appositamente predisposte dall'azienda.
 - rispettando le normative di legge in generale e quelle riportate in questo documento in particolare, nonché le politiche di sicurezza aziendali.
- Il dipendente e le terze parti che utilizzano servizi di internet e posta aziendale in azienda devono quindi:
 - agire nel rispetto della legge, con particolare riferimento alle norme in materia di reati informatici
 - seguire le regole in materia di utilizzo corretto di internet e posta elettronica conosciute come 'Netiquette' e le raccomandazioni aziendali tese ad evitare comportamenti scorretti.

L'azienda si riserva il diritto di impedire l'accesso ad alcuni siti internet ritenuti pericolosi per motivi di sicurezza e per conformità alla legislazione (prevenzione di reato).

I comportamenti palesemente scorretti da parte di un utente, quali:

- violare la sicurezza di archivi e computer della rete
- violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata
- compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan, ecc.) costruiti appositamente;

costituiscono dei veri e propri crimini informatici, come tali punibili anche dalla legge.

11. Utilizzo per ragioni personali di Internet e Posta elettronica

Compatibilmente con la propria attività lavorativa, è consentito utilizzare i servizi di posta elettronica o di rete anche per ragioni personali, purché tale utilizzo:

- avvenga nel rispetto della legge
- sia senza fini di lucro personale
- non violi alcuna regola di sicurezza aziendale

Va comunque tenuto presente che l'azienda non può garantire a priori la riservatezza di comunicazioni personali e che il dipendente può trovarsi a dover rispondere dell'utilizzo, se scorretto, delle risorse messe a disposizione dall'azienda per fini di lavoro.

E' comunque vietato ai singoli dipendenti l'uso, per motivi personali, di servizi a pagamento che prevedano una fatturazione nei confronti dell'Azienda, salvo esplicita autorizzazione della Direzione.

12. Registrazioni di sicurezza

I sistemi informatici aziendali sono soggetti a registrazioni di sicurezza, in base alle esigenze aziendali, alle politiche di sicurezza in vigore ed in conformità alle disposizioni di legge.

Per garantire la manutenzione della sicurezza e della rete, le funzioni aziendali competenti effettuano controlli anche saltuari od occasionali sugli apparati, sui sistemi e sul traffico in rete.

Il fine di tale attività è comunque la rilevazione di possibili anomalie di utilizzo e la fornitura di un adeguato livello di servizio e non il controllo delle attività dei singoli dipendenti.

m) PROCEDURA PER IL CONTROLLO PERIODICO DEL SOFTWARE INSTALLATO

Scopo

Scopo della presente procedura è garantire che in azienda non sia utilizzato software acquisito in modo improprio o illegittimo.

Si dà incarico a InfoCamere di attuare la procedura effettuando le verifiche.

Passi procedurali

Tempistica : ogni 6 mesi

InfoCamere	1	Censisce il software installato sui pc utilizzando il software in dotazione
	2	Incrocia i dati con quelli risultanti dall'inventario delle licenze regolarmente acquisite
	3	Trasmette al dipendente a cui il pc è stato assegnato, e per conoscenza anche al suo Responsabile, l'elenco del software presente su ogni pc per il quale non si gestisce la relativa licenza
Dipendente	4	Ricevuto l'elenco, verifica se: <ul style="list-style-type: none">- la licenza sia stata acquisita direttamente;- il software sia utilizzato grazie a licenza freeware o shareware;- il software goda di una licenza open source;
	5	Dà riscontro di ciò a InfoCamere a e per conoscenza al suo Responsabile
	6	Qualora non rientri nei casi sopraddetti, il dipendente provvede alla cancellazione immediata del software o, qualora esso sia necessario all'attività aziendale, dà avvio alle procedure di acquisizione legittima della licenza
InfoCamere	7	Tiene memoria delle indicazioni fornite dal dipendente sul titolo con cui il software è acquisito e utilizzato

n) PROCEDURA DI GESTIONE DEI RIFIUTI

La presente procedura descrive le modalità di gestione dei rifiuti prodotti da Camera Arbitrale per garantire che essa avvenga nel pieno rispetto delle norme a tutela dell'ambiente.

1) Tipi di rifiuti

Camera Arbitrale produce i rifiuti tipici dell'attività d'ufficio.

L'azienda non attua una politica di raccolta differenziata ad eccezione della carta. Per quest'ultima sono messi a disposizione di dipendenti e collaboratori degli specifici raccoglitori.

I rifiuti prodotti da Camera Arbitrale appartengono alle seguenti categorie:

- 160213 apparecchiature fuori uso, contenenti componenti pericolosi, diverso da quelli di cui alle voci 160209 (trasformatori e condensatori contenenti PCB) e 160212 (apparecchiature fuori uso contenenti amianto in fibre libere)
- 160214 apparecchiature fuori uso, diverse da quelle di cui alle voci da 160209 a 160213
- 150101 imballaggi in carta e cartone
- 080318 toner per stampa esauriti, diversi da quelli di cui alla voce 080317 (toner contenenti sostanze pericolose)
- 170405 ferro e acciaio
- 200121 tubi fluorescenti, ed altri rifiuti contenenti mercurio
- 160604 batterie alcaline (tranne 160603 batterie contenenti mercurio)
- 160107 filtri dell'olio
- 130205 scarti di olio minerale per motori, ingranaggi e lubrificazione, non cloburati
- 160216 componenti rimossi da apparecchiature fuori uso, diversi da quelli di cui alla voce 160215 (componenti pericolosi)
- 160601 batterie al piombo
- 160602 batterie al nichel cadmio

2) Raccolta e smaltimento

I rifiuti sono raccolti e smaltiti con le modalità indicate nella tabella che segue.

Tipo di rifiuto	Gestore
<ul style="list-style-type: none">• 160213 apparecchiature fuori uso, contenenti componenti pericolosi, diverso da quelli di cui alle voci 160209 e 160212• 160214 apparecchiature fuori uso, diverse da quelle di cui alle voci da 160209 a 160213	I rifiuti sono gestiti e smaltiti da TecnoServiceCamere che in base al contratto in essere smaltisce le attrezzature hardware da dismettere

<ul style="list-style-type: none"> • 170405 ferro e acciaio • 200121 tubi fluorescenti, ed altri rifiuti contenenti mercurio • 160107 filtri dell'olio • 130205 scarti di olio minerale per motori, ingranaggi e lubrificazione, non cloburati • 150202 assorbenti e materiali filtranti, stracci e indumenti protettivi, contaminati da sostanze pericolose • 160601 batterie al piombo • 160602 batterie al nichel cadmio • 160604 batterie alcaline (tranne 160603) • altri materiali ingombranti (cartoni, legno etc.) 	<p>I rifiuti sono gestiti e smaltiti da TecnoServiceCamere in base al contratto di manutenzione ordinaria e straordinaria stipulato con la Camera di Commercio a favore, tra l'altro, delle aziende speciali</p>
<ul style="list-style-type: none"> • 150101 imballaggi in carta e cartone • 080318 toner per stampa esauriti, diversi da quelli di cui alla voce 080317 	<p>I rifiuti sono gestiti e smaltiti da TecnoServiceCamere in base al contratto di pulizia e smaltimento rifiuti stipulato con la Camera di Commercio a favore, tra l'altro, delle aziende speciali</p>

In via generale gli stessi gestori si occupano della raccolta del materiale presso i singoli uffici, del deposito temporaneo e quindi del conferimento allo smaltitore.

Qualora fossero necessari interventi specifici, i dipendenti e collaboratori di Camera Arbitrale possono rivolgersi al Servizio Logistica e Sicurezza della Camera di Commercio di Milano che provvederà a contattare le strutture competenti.

3) Deposito temporaneo

I rifiuti sono temporaneamente raccolti nel rispetto delle seguenti regole:

- le apparecchiature elettroniche vengono depositate in spazi dedicati all'interno del magazzino;
- carta, cartoni vetro e toner vengono depositati in appositi contenitori chiusi con relativi coperchi presso gli spazi comuni dedicati;
- plastica e secco sono raccolti in appositi sacchi presso gli spazi comuni dedicati.
- tubi fluorescenti, neon, batterie ed olio minerale depositati in spazi dedicati.

4) Registrazione dei certificati di smaltimento rifiuti

Il Servizio Logistica e Sicurezza della Camera di Commercio di Milano si adopera perché i Gestori trasmettano al più presto i certificati di smaltimento prodotti dagli Smaltitori.

Il Servizio Logistica e Sicurezza della Camera di Commercio di Milano archivia tali certificati in modo che siano facilmente rinvenibili.

5) Dichiarazioni/denunce

Il Servizio Logistica e Sicurezza della Camera di Commercio di Milano provvede alle comunicazioni previste dalle disposizioni di legge, per i materiali di propria competenza.

TecnoServiceCamere provvederà alle comunicazioni previste dalle disposizioni di legge, per i materiali di sua competenza:

6) Contratti con outsourcer

Il Servizio Logistica e Sicurezza della Camera di Commercio di Milano in collaborazione con l'Ufficio Acquisti si adopera perché i contratti con gli outsourcer definiscano puntualmente gli oneri (operativi ed amministrativi) in capo a questi ultimi.

PROCEDURA GESTIONE SMALTIMENTO RIFIUTI PERICOLOSI

Camera Arbitrale non ha rifiuti pericolosi da smaltire. Qualora vi fosse la necessità si doterà di apposita procedura

o) PROCEDURA DI VERIFICA DI AFFIDABILITA' DEL PARTNER

Scopo

Scopo della presente procedura è indicare le modalità con cui si effettua la verifica di affidabilità del partner.

Si applica ogni qualvolta si individua un nuovo partner con il quale si intende porre in essere iniziative comuni (collaborazioni, sponsorship...)

Responsabile dell'iniziativa in partnership	1	Richiede la visura camerale allo scopo di verificare la situazione dell'azienda e di identificare soci e amministratori
	2	Richiede documentazione antimafia
	3	Effettua una ricerca su internet allo scopo di verificare se il partner, i soci principali e gli amministratori non siano indagati o imputati.
	4	In caso di partner straniero, acquisisce tutte le informazioni di natura pubblica e privata utili per verificarne la sua affidabilità
	5	Qualora le ricerche abbiano esito negativo, conserva le risultanze della ricerca
	6	Qualora la ricerca evidenzi aspetti che incidono sull'affidabilità del partner informa il Direttore Generale
Direttore Generale	7	Qualora ritenga di procedere, raccoglie ulteriori informazioni sul partner potenziale e informa l'OdV

5. MISURE DI SICUREZZA INFORMATICA

Le misure di sicurezza informatica sono garantite dagli outsourcer. Si veda quindi il capitolo relativo ai vincoli contrattuali con gli outsourcer.

6. MISURE DI PREVENZIONE E PROTEZIONE DELLA SICUREZZA E DELLA SALUTE DEI LAVORATORI

Le misure di prevenzione e protezione della sicurezza e della salute dei lavoratori sono garantite da un outsourcer. Si veda quindi il capitolo relativo ai vincoli contrattuali con gli outsourcer.

7. VINCOLI CONTRATTUALI CHE IMPONGONO AGLI OUTSOURCER L'ADOZIONE DI MISURE A CONTENIMENTO DEL RISCHIO DI REATO

a) Contratto con TecnoServiceCamere per pulizia etc.

La Camera di Commercio di Milano ha stipulato con TecnoServiceCamere un contratto per la fornitura dei servizi di pulizia, disinfestazione, sanificazione, raccolta differenziata e smaltimento dei rifiuti a favore delle proprie sedi, presso le quali è collocata anche la Camera Arbitrale.

In base a tale contratto Tecno Service Camere garantisce lo smaltimento dei rifiuti organici, carta cartoni e toner esausti.

b) Contratto con TecnoServiceCamere per sicurezza sul lavoro

La Camera di Commercio di Milano ha stipulato con TecnoServiceCamere un contratto per l'assistenza in materia di sicurezza e di igiene sul lavoro anche a favore delle aziende speciali, e quindi di Camera Arbitrale.

Per la prestazione di tale servizio TecnoServiceCamere mette a disposizione un team composto da:

- Responsabile del servizio di prevenzione e protezione, RSPP;
- Tecnico laureato specializzato in impianti elettrici e di sicurezza;
- Tecnico diplomato specializzato in prevenzione infortuni e igiene del lavoro;
- Esperto di programmi di formazione e informazione.

Il contratto specifica a titolo esemplificativo le attività che sono affidate a TecnoServiceCamere:

controllo dell'esistenza e della regolarità delle autorizzazioni burocratiche legate alla sicurezza
analisi di nuovi posti di lavoro per valutarne le condizioni di sicurezza e ergonomia
controllo delle condizioni di sicurezza degli impianti
controllo delle condizioni di sicurezza dei locali (prevenzione incendi, evacuazione dei locali, stato dei pavimenti, passaggi, corridoi, illuminazione d'emergenza)
controllo delle condizioni dei locali di lavoro e dei singoli posti di lavoro (igiene del lavoro, ricambi d'aria, eventuali inquinamenti fisici, chimici, salubrità dei locali e benessere termico)
collaborazione con il Medico competente
Visite periodiche nei locali di lavoro
Consulenza sull'acquisizione di nuove attrezzature e macchinari
Predisposizione di procedure interne di sicurezza in merito agli obblighi dei lavoratori, dei preposti e dei dirigenti, comportamenti da tenere da parte degli appaltatori e delle imprese che operano all'interno dei locali di lavoro, rapporti con gli appaltatori anche per quanto attiene le manutenzioni e le necessità manutentive
Rapporti in esito alle nuove valutazioni, contenenti anche gli standard a cui si fa riferimento nelle valutazioni stesse
Collaborazione con i progettisti di nuove opere o interventi
Partecipazione alle riunioni periodiche con i rappresentanti dei lavoratori per la sicurezza

Proporre e controllare misurazioni strumentali del livello di pressione sonora nei locali di lavoro e, se necessario, valutazione del livello di esposizione personale
Proporre e controllare misurazioni strumentali, ove necessarie, del livello di illuminazione ambientale
Proporre e controllare misurazioni strumentali a campione dei dati microclimatici e di benessere termico
Preparare piano di informazioni ai dipendenti sui rischi, sui modi di prevenirli e sui comportamenti
Preparare piano di formazione dei dipendenti sul miglioramento della sicurezza nei luoghi di lavoro
Controllare che sia messo a disposizione e consegnato a tutti i nuovi dipendenti "videoterminalisti" un libretto informativo/formativo sul lavoro al videoterminale
Proporre, coordinare e controllare i piani di analisi strumentale (polveri, rumore, microclima) eventualmente necessari ad accertare le condizioni di inquinamento ambientale
Proporre piani di manutenzione ordinaria e straordinaria legati a problemi di sicurezza
Controllo periodico dello stato di attuazione del piano di miglioramento delle condizioni di sicurezza ed igiene sul posto di lavoro sulla base delle risultanze delle valutazioni effettuate
Mette a disposizione un presidio medico/infermieristico presso la sede di via meravigli
Far effettuare le visite mediche periodiche obbligatorie specialistiche e richieste

La redazione del Documento di Valutazione dei Rischi è affidato all'RSPP.

c) Contratto con Infocamere

Il contratto prevede la gestione dei seguenti servizi con le conseguenti misure di sicurezza:

- Gestione servizi in outsourcing Server farm
- Gestione e supporto rete IP
- Gestione e manutenzione Posta elettronica
- Manutenzione intranet

d) Contratto con Infocamere

Infocamere offre servizi di connettività locale e geografica. Nell'ambito di tale contratto garantisce l'adozione di una serie di misure di sicurezza della rete

Misure di sicurezza della rete di connettività locale e geografica

Le misure relative alla sicurezza della rete di connettività locale e geografica sono garantite da Infocamere che, nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) adottato, assicura l'applicazione di:

- misure organizzative, che comprendono i processi di gestione della Sicurezza delle Informazioni, di Tutela dei dati Personali, di definizione delle Politiche e del Piano della Sicurezza
- misure logiche che comprendono i processi di gestione del sistema di Identity Management e di sicurezza degli accessi logici per le applicazioni ed i servizi
- misure tecnologiche che comprendono i processi di gestione ed evoluzione degli strumenti tecnologici, quali: Firewall, Proxy, VPN, IPS.

Qui di seguito si riportano per sommi capi le misure adottate. Per il dettaglio si rimanda

Modello di Organizzazione, Gestione e Controllo per la prevenzione dei reati (D.lgs. 231/2001)

Allegato 3 – Descrizione delle misure a contenimento del rischio di reato

Approvato in data 22.06.2020

al contratto con Infocamere:

Monitoraggio della sicurezza della rete	Attività di controllo sull'infrastruttura e si segnalano incidenti di sicurezza e attività anomale
Identity/Access Management	Sistema centralizzato, basato su server RADIUS, per la gestione delle credenziali di tutte le persone autorizzate ad accedere a vario titolo agli apparati di gestione ed esercizio della rete. Ogni operatore abilitato è dotato di credenziali personali e univoche, per permettere il tracciamento degli accessi effettuati e garantire che gli operatori possano svolgere operazioni esclusivamente sulle informazioni e sulle risorse cui essi sono autorizzati e di cui hanno necessità.
Intrusion Detection/Prevention System	Infrastruttura Hardware/Software per l'Intrusion Prevention con l'obiettivo di identificare in tempo reale di possibili attacchi ed il blocco automatico del traffico di rete identificabile con certezza come doloso.
Proxy	il servizio di Proxy effettua e garantisce: <ul style="list-style-type: none">• l'autenticazione degli utenti che accedono a internet, mediante richiesta di credenziali personali• il logging dei dati di traffico, secondo la normativa di contrasto alla criminalità e nel rispetto delle indicazioni del Garante alla Privacy;• un sistema di filtraggio preventivo della navigazione, secondo policies definibili per gruppi di dipendenti, in ottemperanza a quanto raccomandato dal Garante e alle politiche in vigore presso la CCIAA di Milano.• un sistema di filtraggio preventivo antivirus.
Sicurezza VPN	un sistema di autenticazione (che diventa autenticazione forte per i profili di accesso non limitati a risorse WEB) integrato con ISEC, il sistema di Identity Management di InfoCamere per le CCIAA <ul style="list-style-type: none">• profili di accesso diversificati in base alle esigenze• log centralizzato degli accessi

Allegati

Allegato Regolamenti e Vademecum arbitrato e conciliazione

- **Regolamento arbitrale**
- **Regolamento di mediazione**
- **Regolamento di mediazione internazionale**
- **Regolamento di mediazione telematica**
- **Regolamento dell'Italy China Business Mediation Center**
- **Regolamento per la risoluzione delle dispute nel country code Top Level Domain "it"**
- **Regolamento per il servizio Risolvionline**
- **Regolamento Dispute Resolution Board**
- **Vademecum per il servizio di Conciliazione**

Allegato Processo degli Acquisti

Allegato Regolamento Contabile

Allegato Procedura adempimenti fiscali

Allegato Regolamento per le sponsorizzazioni

Allegato Manuale di utilizzo Gedoc

Allegato Provvedimento di approvazione del regolamento interno per la selezione di personale per rapporto di lavoro dipendente

Allegato Regolamento per il conferimento di incarichi ad esperti esterni alla Camera Arbitrale

Allegato Rimborso spese viaggi

Allegato Procedura Carte di credito aziendali