Mediacom Customer Operations Process	**Sistema di Gestione per la Sicurezza delle Informazioni**

La Politica della Sicurezza delle Informazioni

[x] **COPIA SOGGETTA A REV. N°** 01	[ ] **COPIA NON SOGGETTA A REV. N°** ……
Distribuita a [(1)]: TUTTI **il: 15/03/2019**	**Distribuita a:** **il:**

[(1)] Il destinatario è pregato di firmare e restituire la fotocopia di questa pagina, oppure di firmare la lista di distribuzione conservata da RQ.

- [ ] **Manuale**
- [x] **Procedure**
- [ ] **Modulistica**
- [ ] **Documento**

REDAZIONE, VERIFICA, APPROVAZIONE

REDAZIONE	RCC.
VERIFICA	RGQ
APPROVAZIONE	DG

STATO DELLE REVISIONI

REV. N.	PARAGRAFI REVISIONATI	DESCRIZIONE REVISIONE	DATA
01	TUTTO	TUTTO	15/03/2019

ELENCO ALLEGATI

ALL. N.	CODICE	DESCRIZIONE ALLEGATO	REV. N.

INDICE

1. LA POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

1.1 SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni attuati da Mediacom srl al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

1.2 DESCRIZIONE

La **Mediacom s.r.l.** considera come obiettivo primario, per la sicurezza delle informazioni, la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa e la loro gestione.
Ciò significa implementare e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'SGSI (ISMS), attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi strutturali associati quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità**: garantire una provenienza affidabile dell'informazione.
6. **Privacy**: garantire la protezione ed il controllo dei dati personali

Nell'ambito della gestione dei servizi offerti da **Mediacom s.r.l.,** attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti, seguendo i requisiti specificati della Norma ISO 27001:2013, l'implementazione dell'SGSI (ISMS), assicura:

· la garanzia, per le Aziende Committenti, di aver scelto un partner affidabile per il trattamento del proprio patrimonio informativo;
· un'elevata immagine aziendale;
· la completa osservanza delle Service Level Agreement stabilite con i clienti;
· la soddisfazione del cliente;
· il rispetto delle normative vigenti e degli standard internazionali di sicurezza

1.3 AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di **Mediacom s.r.l.,** si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi e nelle diverse sedi aziendali.

1.4 POLITICA DELLA DIREZIONE

Premesso che Il raggiungimento di adeguati livelli di sicurezza delle informazioni consente all'azienda di mitigare e contrastare perdite e danneggiamenti che possano avere impatto sulle persone, sull'immagine e la reputazione aziendali, sugli aspetti di natura economica e finanziaria, oltre a consentire la conformità al contesto contrattuale e legislativo vigente in materia di protezione delle informazioni, la **Direzione** esprime il proprio impegno nell'implementare, sviluppare e promuovere una efficace Governance del Sistema di Gestione per la Sicurezza delle Informazioni, identificando i seguenti **obiettivi**:

- il miglioramento continuo del sistema di gestione per la sicurezza dei dati e delle informazioni;
- la valutazione dei rischi relativi alla gestione dei dati e delle informazioni con particolare attenzione alle minacce che possono impattare su: riservatezza, integrità e disponibilità del dato;

- l'applicazione sistematica dei requisiti di Legge cogenti e ogni altro requisito/norma/regolamento significativo in ambito sicurezza dei dati e delle informazioni;
- l'impegno finalizzato alla prevenzione di eventi negativi in materia di sicurezza dei dati e delle informazioni (es. sottrazione, perdita, violazione del dato);
- il consolidamento dei rapporti di collaborazione con tutte le parti interessate per garantire il miglioramento continuo delle performance del Sistema di gestione;
- la formazione ed informazione continua del personale e, ove opportuno, dei fornitori/collaboratori/clienti sui rischi relativi ad un'errata gestione dei dati e delle informazioni;
- la soddisfazione del cliente.
- assegnare le risorse necessarie al fine di assicurare l'impiego di misure idonee per gli aspetti riguardanti la sicurezza fisica, logica ed organizzativa;

La continua crescita del livello di servizio verrà perseguita mediante il regolare riesame dello stesso, volto al monitoraggio degli obiettivi prestabiliti e al riconoscimento di eventuali aree di miglioramento.
Le esigenze e le aspettative del cliente vengono soddisfatte attraverso il massimo impegno nelle attività di esecuzione dei servizi erogati.
La Direzione, inoltre, si impegna ad attuare, sostenere e verificare periodicamente la Politica di cui sopra e a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa.
In occasione di ogni Riesame della Direzione, gli obiettivi e la Politica del Sistema di gestione sulla sicurezza sono riesaminati per accertarne la continua idoneità.
La corretta ed efficiente implementazione del sistema di gestione e la sua revisione, in conformità a quanto richiesto dalla Norma ISO IEC 27001, è affidata al Responsabile Area ICT.

1.5 RUOLI E RESPONSABILITA'

L'efficace attuazione del SGSI (ISMI ed il conseguimento degli obiettivi prefissati sono assicurati dall'assetto organizzativo definito e messo in atto dalla **Direzione**. A tale scopo, essa identifica, definisce ed assegna l'insieme dei ruoli e delle responsabilità relative al Sistema di Gestione della Sicurezza delle Informazioni di Mediacom srl e li comunica rendendoli disponibili a tutti i dipendenti all'interno della rete aziendale. Di seguito vengono sinteticamente riportati i ruoli, le principali prerogative e responsabilità:

Direzione Generale - determina la strategia dell'organizzazione integrata con il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), stabilisce gli obiettivi di sicurezza delle informazioni e mette a disposizione le risorse necessarie per la gestione del SGSI. Inoltre promuove il miglioramento continuo del SGSI, esegue il riesame e valuta le prestazioni del SGSI.

Steering Committee - fornisce il supporto decisionale al Responsabile del SGSI, supporta l'integrazione del SGSI all'interno dei processi aziendali. Supporta la Direzione nel riesame del SGSI.

Responsabile del SGSI – è responsabile dell'implementazione e della gestione complessiva del Sistema di Gestione della Sicurezza delle Informazioni attraverso le risorse messe a disposizione dalla Direzione nel rispetto dei requisiti delle parti interessate e per il raggiungimento degli obiettivi stabiliti. È parte attiva nei processi di validazione ed approvazione di policy e procedure del SGSI.

Risorse Umane - misura e gestisce il grado di competenza e consapevolezza delle risorse umane coinvolte nel sistema di gestione definendo appositi programmi di sensibilizzazione e formazione e garantendone l'esecuzione.

Risk Owner – gestisce uno o più rischi specifici. Approva il piano di trattamento del rischio in collaborazione con il Responsabile SGSI, sulla base della soglia di accettabilità stabilità dalla Direzione Generale. È responsabile dell'accettazione formale del rischio residuo.

Asset Owner – garantisce la sicurezza delle informazioni dell'asset di cui è l'owner. Tale governo è garantito rispettando le policy del sistema di gestione, i processi e le procedure di sicurezza associate agli asset oltre che mediante l'applicazione di opportuni controlli determinati in collaborazione con il Responsabile SGSI. Stabilisce le regole di accesso all'asset e collabora ai controlli di sicurezza da applicare ad esso al fine di ridurre rischi identificati dal risk owner fino al livello accettabile.

2. IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

La gestione del sistema di sicurezza informatica si articola, principalmente, nelle seguenti tematiche:

- Analisi e valutazione dei rischi;
- Attività di conoscenza e monitoraggio delle minacce relative mirate al contesto aziendale che permetta una gestione del rischio adeguata allo stesso;
- Selezionare, progettare e implementare misure di mitigazione dei rischi di sicurezza;
- Garantire e verificare l'efficacia dei controlli di sicurezza;
- Riesaminare l'adeguatezza dei controlli e l'efficacia del sistema di protezione dell'informazione per assicurare il suo continuo mantenimento e miglioramento.

2.1 IDENTIFICAZIONE, ANALISI E VALUTAZIONE DEL RISCHIO

Al fine di garantire un'adeguata protezione, vengono eseguite attività di selezione dei requisiti, implementazione, manutenzione, verifica e miglioramento dei controlli, seguendo un approccio basato sul rischio e assicurando l'adozione di best practice disponibili per garantire la conformità alla legislazione pertinente in materia di elaborazione dell'informazione.
L'approccio basato sul rischio viene definito tramite metodologie e strumenti atti a identificare, valutare e trattare i rischi in ambito di Information Security e di Cyber Security.
Le attività di trattamento dei rischi vengono monitorate attraverso il Piano di Trattamento dei Rischi di Sicurezza mentre il documento SoA (Statement of Applicability) fornisce l'insieme dei controlli di sicurezza applicabili al contesto aziendale

2.2 FORMAZIONE

La cultura della Sicurezza delle Informazioni è considerata un valore fondamentale per l'Azienda e viene promossa attraverso un processo continuativo di formazione e aggiornamento.
La Mediacom realizza il proprio programma di sensibilizzazione attraverso sessioni formative multimediali, test ed esercitazioni, partecipazione a corsi specifici di formazione e ulteriori iniziative utili a diffondere la conoscenza e la consapevolezza in materia di sicurezza all'interno dell'azienda.
Tutto il personale riceve una formazione periodica sulla sicurezza delle informazioni, adeguata alle proprie attività quotidiane e alla loro funzioni.

2.3 LINEE GUIDA DI SICUREZZA E CONTINUITA' OPERATIVA

Mediacom ha predisposto un sistema documentale sui temi della sicurezza che si articola in Politica della Sicurezza, Linee Guida di Sicurezza e di Continuità Operativa e Procedure.
La formalizzazione dei requisiti di Sicurezza e l'articolazione della relativa documentazione su più livelli consente ed assicura la definizione e l'indicazione dei presidi e controlli in relazione alle singole attività lavorative.
Esse, sono definite in conformità ai controlli della normativa ISO/IEC 27001, alla regolamentazione nell'ambito della Protezione dei Dati Personali e ad altre best practice di settore applicabili e regolarmente riesaminate alla luce dei risultati dell'analisi dei rischi e degli aggiornamenti normativi.
Inoltre forniscono i criteri, i requisiti e i controlli per garantire l'efficacia degli obiettivi della Politica della Sicurezza delle Informazioni.

2.4 PERSONALE E SICUREZZA

Le persone costituiscono un fattore di successo per costruire una efficace sicurezza delle informazioni in azienda.
Nelle fasi di selezione ed inserimento del personale, devono essere valutati i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza aziendale in funzione delle attività che dovranno essere svolte.
Durante la permanenza in Mediacom srl il personale deve ricevere un'adeguata e continuativa formazione inerente alle tematiche di sicurezza dei dati.
Vengono definiti specifici criteri e controlli con l'obiettivo di contrastare i rischi introdotti dalla scarsa conoscenza e consapevolezza delle persone circa le tematiche di sicurezza e continuità operativa.
Questi criteri devono essere applicati dalle funzioni aziendali che hanno la responsabilità di gestire le risorse umane, stabilendone le modalità lavorative, i ruoli, la formazione, gli strumenti di lavoro e le valutazioni durante tutto il loro ciclo lavorativo

2.5 IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DELLE RISORSE

Deve esistere ed essere mantenuto aggiornato, nel corso del tempo, un sistema di censimento di tutti i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
Ogni risorsa (bene materiale/immateriale) deve essere direttamente associabile ad un responsabile.
Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati. La criticità delle informazioni deve essere valutata in maniera quanto più oggettiva possibile, attraverso l'utilizzo di adeguate metodologie di lavoro.
Le modalità di gestione ed i sistemi di protezione per le informazioni e gli asset su cui risiedono devono essere coerenti con il livello di criticità identificato.

2.6 GESTIONE SICURA DEGLI ACCESSI LOGICI

L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti (c.d. principio del "need-to-know"). La comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.
L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi.
Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione.
E' necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
I sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

2.7 NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE AZIENDALI

Gli ambienti di lavoro e le risorse aziendali devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate.
Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo.
I sistemi informatici aziendali devono essere impiegati da dipendenti e dai collaboratori secondo procedure approvate.

2.8 GESTIONE DEGLI EVENTI ANOMALI E DEGLI INCIDENTI

Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e secondo adeguate procedure, eventuali problematiche legate alla sicurezza delle informazioni.
Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.
Deve esistere un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate.

2.9 GESTIONE DELLA SICUREZZA FISICA

Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite:

- l'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate;
- la definizione dei livelli adeguati di protezione.

Deve essere garantita la sicurezza delle apparecchiature tramite:

- la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;
- la messa a disposizione delle risorse necessarie al loro funzionamento;
- la predisposizione di un adeguato livello di manutenzione.

2.10 ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI

Gli accordi con le terze parti e con gli outsourcer che accedono alle informazioni/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza.
Gli accordi con terze parti e con gli outsourcer, ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali Regolamento UE 2016/ 679 ("normativa privacy").

2.11 GESTIONE DELLA BUSINESS CONTINUITY

Devono essere attentamente identificati e valutati, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business.
Deve essere predisposto un piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative sulla missione aziendale.
Devono essere preparate, validate e opportunamente divulgate tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità.
Devono essere periodicamente effettuati i test per tutti i componenti del piano di continuità.
Deve essere assicurato il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

2.12 MONITORAGGIO, TRACCIAMENTO E VERIFICHE TECNICHE

I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato.
A fronte dei risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative.
Devono essere pianificate attività periodiche di audit del sistema di gestione della sicurezza delle informazioni.

2.13 CICLO DI VITA DEI SISTEMI E DEI SERVIZI

Nella fase di progettazione e sviluppo devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:

- inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e sistemi;
- adozione di best practice per lo sviluppo e la manutenzione del software;
- gestione controllata della documentazione;
- separazione degli ambienti di sviluppo e test con impiego di procedure formali di accettazione nel passaggio fra ambienti.

Nella fase di esercizio devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:

- capacity management dell'infrastruttura tecnologica;
- securizzazione dei sistemi e dei dati (configuration management, hardening,installazione di sistemi anti-malware, crittografia);
- utilizzo di procedure di change management;
- adozione di procedure di backup e restore;
- adozione di procedure di dismissione controllata dei sistemi (per esempio cancellazione sicura dei dischi);
- network security: segregazione delle reti, monitoraggio dei gateway(firewall).

Nella gestione dei servizi devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:

- monitoraggio dei sistemi e servizi;
- gestione utenze;
- performance monitoring.

2.14 RISPETTO DELLA NORMATIVA

Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi.
I responsabili delle diverse aree devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati e rispettati.

3 DEFINIZIONE DEI RUOLI E DELLE RESPONSABILITÀ

3.1 STRUTTURA RESPONSABILE DELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

La struttura responsabile del sistema di gestione della sicurezza delle informazioni dovrà farsi promotrice, al fine di rendere la politica generale di sicurezza coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo e legislativo in materia di sicurezza delle informazioni;
- risultati di analisi sui costi, impatti, efficacia ed efficienza del sistema di gestione per la sicurezza delle informazioni.

3.2 COMITATO DEI RESPONSABILI

Il Comitato dei Responsabili è l'organismo a cui competono, con il supporto della struttura responsabile del sistema di gestione della sicurezza delle informazioni, le decisioni di massimo livello riguardo alle tematiche di sicurezza.
In particolare ha la responsabilità di supportare e garantire l'applicazione delle politiche generali del Sistema di Gestione della Sicurezza delle Informazioni, di definire le politiche idonee di gestione del rischio e di supportare costantemente il processo di sensibilizzazione sulle tematiche di sicurezza.