

CONTROLLO ISO 27001	FASI DI IMPLEMENTAZIONE	ATTIVITÀ	CONFORME?	NOTE
5	Politiche di sicurezza delle informazioni			
5.1	Direttive manageriali per la sicurezza delle informazioni			
5.1.1	Politiche di sicurezza delle informazioni	Sono state definite politiche della sicurezza?		
		Tutte le politiche sono state approvate dai vertici dirigenziali?		
		La conformità è documentata?		
6	Organizzazione della sicurezza delle informazioni			
6.1	Ruoli e responsabilità per la sicurezza delle informazioni			
6.1.1	Ruoli e responsabilità per la sicurezza	I ruoli e le responsabilità sono stati definiti?		
6.1.2	Separazione delle mansioni	Le mansioni sono state correttamente assegnate a persone diverse?		
6.1.3	Contatto con le autorità	È stato contattato l'ente / l'autorità che deve effettuare la verifica della conformità?		
6.1.4	Contatto con i gruppi di interesse speciale	Sono stati contattati i gruppi di interesse speciali che si occupano di conformità?		
6.1.5	Sicurezza delle informazioni nella gestione dei progetti	La sicurezza delle informazioni nella gestione dei progetti è documentata?		
6.2	Dispositivi mobili e telelavoro			
6.2.1	Politica per i dispositivi mobili	È stata definita una politica per i dispositivi mobili?		
6.2.2	Telelavoro	È stata definita una politica per il lavoro a distanza?		

7	Sicurezza nelle risorse umane			
7.1	Prima dell'assunzione			
7.1.1	Valutazione	È stata definita una politica per la valutazione dei dipendenti prima dell'assunzione?		
7.1.2	Termini e condizioni di impiego	È stata definita una politica HR per i termini e le condizioni di impiego?		
7.2	Durante il periodo di lavoro			
7.2.1	Responsabilità dirigenziali	È stata definita una politica che stabilisca le responsabilità a livello dirigenziale?		
7.2.2	Sensibilizzazione e formazione in materia di sicurezza delle informazioni	È stata definita una politica per la sensibilizzazione e la formazione in materia di sicurezza delle informazioni?		
7.2.3	Procedimenti disciplinari	È stata definita una politica per i procedimenti disciplinari in materia di sicurezza delle informazioni?		
7.3	Cessazione e modifica del rapporto di lavoro			
7.3.1	Responsabilità in caso di cessazione o di modifica del rapporto di lavoro	È stata definita una politica in materia di sicurezza delle informazioni in caso di cessazione o di modifica del rapporto di lavoro?		
8	Gestione degli asset			
8.1	Responsabilità per gli asset			
8.1.1	Inventario degli asset	Elenco completo degli asset inventariati?		
8.1.2	Proprietà degli asset	Elenco completo della proprietà degli asset		
8.1.3	Uso accettabile degli asset	È stata definita uso accettabile degli asset		
8.1.4	Reso degli asset	È stata definita una politica per il reso degli asset?		

8.2	Classificazione delle informazioni			
8.2.1	Classificazione delle informazioni	È stata definita una politica per la classificazione delle informazioni.		
8.2.2	Etichettatura delle informazioni	È stata definita una politica per l'etichettatura delle informazioni?		
8.2.3	Gestione degli asset	È stata definita una politica per la gestione degli asset?		
8.3	Gestione dei media			
8.3.1	Gestione dei supporti multimediali rimovibili	È stata definita una politica per la gestione dei supporti multimediali rimovibili?		
8.3.2	Smaltimento dei supporti multimediali	È stata definita una politica per lo smaltimento dei supporti multimediali?		
8.3.3.	Trasferimento dei supporti multimediali fisici	È stata definita una politica per il trasferimento dei supporti multimediali fisici?		
9	Controllo degli accessi			
9.1	Responsabilità per gli asset			
9.1.1	Politica di controllo degli accessi	È stata definita una politica per il controllo degli accessi?		
9.1.2	Accesso alle reti e ai servizi di rete	È stata definita una politica per l'accesso alle reti e ai servizi di rete?		
9.2	Responsabilità per gli asset			
9.2.1	Registrazione degli asset degli utenti e annullamento della registrazione	È stata definita una politica per la registrazione e l'annullamento della registrazione degli asset degli utenti?		
9.2.2	Provisioning degli accessi degli utenti	È stata definita una politica per il provisioning degli accessi degli utenti?		

9.2.3	Gestione dei diritti di accesso con privilegi	È stata definita una politica per la gestione dei diritti di accesso con privilegi?		
9.2.4	Gestione delle informazioni di autenticazione segrete degli utenti	È stata definita una politica per la gestione delle informazioni di autenticazione segrete degli utenti?		
9.2.5	Revisione dei diritti di accesso degli utenti	È stata definita una politica per la revisione dei diritti di accesso degli utenti?		
9.2.6	Rimozione o adeguamento dei diritti di accesso	È stata definita una politica per la rimozione o l'adeguamento dei diritti di accesso?		
9.3	Responsabilità degli utenti			
9.3.1	Utilizzo delle informazioni di autenticazione segrete	È stata definita una politica per l'utilizzo delle informazioni di autenticazione segrete?		
9.4	Controllo degli accessi ai sistemi e alle applicazioni			
9.4.1	Limitazioni di accesso alle informazioni	È stata definita una politica per le limitazioni di accesso alle informazioni?		
9.4.2	Procedure di log-in sicuro	È stata definita una politica per le procedure di log-in sicuro?		
9.4.3	Sistemi di gestione delle password	È stata definita una politica per i sistemi di gestione delle password?		
9.4.4	Utilizzo di programmi di utility con privilegi	È stata definita una politica per l'utilizzo di programmi di utility con privilegi?		
9.4.5	Controllo degli accessi al codice sorgente del programma	È stata definita una politica per il controllo degli accessi al codice sorgente del programma?		
10	Crittografia			
10.1	Controlli di crittografia			
10.1.1	Politica sull'utilizzo dei controlli di crittografia	È stata definita una politica per l'utilizzo dei controlli di crittografia?		
10.1.2	Gestione delle chiavi	È stata definita una politica per la gestione delle chiavi?		

11	Sicurezza fisica e ambientale			
11.1	Aree protette			
11.1.1	Sicurezza fisica perimetrale	È stata definita una politica per la sicurezza fisica perimetrale?		
11.1.2	Controlli degli ingressi fisici	È stata definita una politica per i controlli degli ingressi fisici?		
11.1.3	Messa in sicurezza degli uffici, delle sale e delle infrastrutture	È stata definita una politica per la messa in sicurezza degli uffici, delle sale e delle infrastrutture?		
11.1.4	Protezione dalle minacce esterne e ambientali	È stata definita una politica per la protezione dalle minacce esterne e ambientali?		
11.1.5	Lavoro nelle aree protette	È stata definita una politica per accedere alle aree protette?		
11.1.6	Aree di consegna e carico	È stata definita una politica per le aree di consegna e carico?		
11.2	Apparecchiature			
11.2.1	Protezione delle apparecchiature e loro ubicazione in luoghi sicuri	È stata definita una politica per la protezione delle apparecchiature e per la loro ubicazione in luoghi sicuri?		
11.2.2	Servizi di supporto	È stata definita una politica per i servizi di supporto?		
11.2.3	Sicurezza dei cablaggi	È stata definita una politica per la sicurezza dei cablaggi?		
11.2.4	Manutenzione delle apparecchiature	È stata definita una politica per la manutenzione delle apparecchiature?		
11.2.5	Eliminazione degli asset	È stata definita una politica per l'eliminazione degli asset?		
11.2.6	Sicurezza delle apparecchiature e degli asset off-premises	È stata definita una politica per la sicurezza delle apparecchiature e degli asset off-premises?		

11.2.7	Smaltimento sicuro o riutilizzo delle apparecchiature	È stata definita una politica per lo smaltimento sicuro o il riutilizzo delle apparecchiature?		
11.2.8	Apparecchiature degli utenti non presidiate	È stata definita una politica per le apparecchiature degli utenti non presidiate?		
11.2.9	Politica "clear desk" e "clear screen"	È stata definita una politica "clear desk" e "clear screen"?		
12	<i>Sicurezza delle operazioni</i>			
12.1	Procedure operative e responsabilità			
12.1.1	Procedure operative documentate	È stata definita una politica per le procedure operative documentate?		
12.1.2	Gestione delle modifiche	È stata definita una politica per la gestione delle modifiche?		
12.1.3	Gestione della capacità	È stata definita una politica per la gestione della capacità?		
12.1.4	Separazione tra ambiente di sviluppo, di test e operativo	È stata definita una politica per la separazione tra ambiente di sviluppo, di test e operativo?		
12.2	Protezione da malware			
12.2.1	Controlli antimalware	È stata definita una politica per i controlli antimalware?		
12.3	Backup di sistema			
12.3.1	Backup	È stata definita una politica per il backup dei sistemi?		
12.3.2	Backup delle informazioni	È stata definita una politica per il backup delle informazioni?		
12.4	Registrazione e monitoraggio			
12.4.1	Registrazione degli eventi	È stata definita una politica per la registrazione degli eventi?		

12.4.2	Protezione delle informazioni dei registri	È stata definita una politica per la protezione delle informazioni dei registri?		
12.4.3	Registri amministrativi e operativi	È stata definita una politica per i registri amministrativi e operativi?		
12.4.4	Sincronizzazione dell'orologio di sistema	È stata definita una politica per la sincronizzazione dell'orologio di sistema?		
12.5	Controllo del software operativo			
12.5.1	Installazione di software nei sistemi operativi	È stata definita una politica per l'installazione di software nei sistemi operativi?		
12.6	Gestione delle vulnerabilità tecniche			
12.6.1	Gestione delle vulnerabilità tecniche	È stata definita una politica per la gestione delle vulnerabilità tecniche?		
12.6.2	Restrizioni all'installazione di software	È stata definita una politica per le restrizioni all'installazione di software?		
12.7	Considerazioni sull'audit dei sistemi informativi			
12.7.1	Controllo degli audit dei sistemi informativi	È stata definita una politica per il controllo degli audit dei sistemi informativi?		
13	Sicurezza delle comunicazioni			
13.1	Gestione della sicurezza di rete			
13.1.1	Controlli di rete	È stata definita una politica per i controlli di rete?		
13.1.2	Sicurezza dei servizi di rete	È stata definita una politica per la sicurezza dei servizi di rete?		
13.1.3	Segmentazione delle reti	È stata definita una politica per la segmentazione delle reti?		
13.2	Trasferimento delle informazioni			
13.2.1	Criteri e procedure di trasferimento delle informazioni	È stata definita una politica per i criteri e le procedure di trasferimento delle informazioni?		

13.2.2	Accordi sul trasferimento delle informazioni	È stata definita una politica per stipulare accordi sul trasferimento delle informazioni?		
13.2.3	Messaggistica elettronica	È stata definita una politica per la messaggistica elettronica?		
13.2.4	Accordi di riservatezza e non divulgazione	È stata definita una politica per gli accordi di riservatezza e non divulgazione?		
13.2.5	Acquisizione, sviluppo e manutenzione dei sistemi	È stata definita una politica per l'acquisizione, lo sviluppo e la manutenzione dei sistemi?		
14	<i>Acquisizione, sviluppo e manutenzione dei sistemi</i>			
14.1	Requisiti di sicurezza dei sistemi informativi			
14.1.1	Analisi e specifiche dei requisiti di sicurezza delle informazioni	È stata definita una politica per l'analisi e le specifiche dei requisiti di sicurezza delle informazioni?		
14.1.2	Protezione dei servizi delle applicazioni sulle reti pubbliche	È stata definita una politica per proteggere i servizi delle applicazioni sulle reti pubbliche?		
14.1.3	Protezione delle transazioni dei servizi delle applicazioni	È stata definita una politica per proteggere le transazioni dei servizi delle applicazioni?		
14.2	Sicurezza nei processi di sviluppo e supporto			
14.2.1	Sviluppo interno	È stata definita una politica per lo sviluppo interno?		
15	<i>Relazioni con i fornitori</i>			
15.1.1	Relazioni con i fornitori	È stata definita una politica per le relazioni con i fornitori?		
16	<i>Gestione degli incidenti di sicurezza delle informazioni</i>			
16.1.1	Gestione della sicurezza delle informazioni	È stata definita una politica per la gestione della sicurezza delle informazioni?		

17	Aspetti della sicurezza delle informazioni nella gestione della continuità operativa			
17.1	Continuità della sicurezza delle informazioni			
17.1.1	Continuità della sicurezza delle informazioni	È stata definita una politica per la continuità della sicurezza delle informazioni?		
17.2	Ridondanze			
17.2.1	Ridondanze	È stata definita una politica delle ridondanze?		
18	Conformità			
18.1	Conformità agli obblighi legali e contrattuali			
18.1.1	Identificazione degli obblighi legali e contrattuali applicabili	È stata definita una politica per l'identificazione degli obblighi legali e contrattuali applicabili?		
18.1.2	Diritti di proprietà intellettuale	È stata definita una politica per i diritti di proprietà intellettuale?		
18.1.3	Protezione dei record	È stata definita una politica per la protezione dei record?		
18.1.4	Privacy e protezione dei dati personali (PII)	È stata definita una politica per la privacy e la protezione dei dati personali (PII)?		
18.1.5	Regolamentazione dei controlli di crittografia	È stata definita una politica per la regolamentazione dei controlli di crittografia?		
18.1	Revisione indipendente della sicurezza delle informazioni			
18.1.1	Conformità ai criteri e agli standard di sicurezza	È stata definita una politica per la conformità ai criteri e agli standard di sicurezza?		
18.1.2	Esame della conformità tecnica	È stata definita una politica per l'esame della conformità tecnica?		

DICHIARAZIONE DI NON RESPONSABILITÀ

Qualsiasi articolo, modello o informazione sono forniti da Smartsheet sul sito web solo come riferimento. Pur adoperandoci a mantenere le informazioni aggiornate e corrette, non offriamo alcuna garanzia o dichiarazione di alcun tipo, esplicita o implicita, relativamente alla completezza, l'accuratezza, l'affidabilità, l'idoneità o la disponibilità rispetto al sito web o le informazioni, gli articoli, i modelli o della relativa grafica contenuti nel sito. Qualsiasi affidamento si faccia su tali informazioni, è pertanto strettamente a proprio rischio.