REGIONE SICILIANA

ISTITUTO REGIONALE DEL VINO E DELL'OLIO

IL DIRETTORE GENERALE

D.D.G. Numero **232_**
Data di registrazione **10/06/2025_**

Proposta di Decreto N. 238

OGGETTO : ADOZIONE MANUALE DI GESTIONE DOCUMENTALE VERSIONE 1.0 _

VISTA la L.R. n. 64 del 18 luglio 1950 - Istituzione in Sicilia dell'Istituto Regionale della Vite e del Vino - e successive modifiche ed integrazioni;
VISTO l'art. 35 della L.R. n. 2 dell'8 febbraio 2007 relativo al riconoscimento di questo Istituto quale Ente di Ricerca della Regione Siciliana;
VISTE le delibere del Consiglio di Amministrazione dell'Ente n. 107 del 1 ottobre 2009 e n. 3 del 22 gennaio 2010 con le quali è stato approvato il Regolamento di Organizzazione;
VISTO l'art. 16 della L.R. n. 25 del 24 novembre 2011 che estende le competenze dell'ente al settore oleario attribuendogli la nuova denominazione di Istituto Regionale del Vino e dell'Olio;
VISTA la deliberazione della Giunta Regionale n. 327 dell'11/10/2024, con la quale l'avv. Giuseppa Mistretta, Funzionario avvocato della Regione Siciliana, viene nominata Commissario straordinario dell'Istituto Regionale del Vino e dell'Olio (I.R.V.O.), con i poteri di Presidente e del Consiglio di Amministrazione fino all'insediamento degli organi ordinari di amministrazione, in conformità alla proposta dell'Assessore regionale per l'agricoltura, lo sviluppo rurale e la pesca mediterranea, di cui alla nota 11 settembre 2024, prot. n. 7695/GAB, e relativi atti acclusi, come integrata dalla nota 18 settembre 2024, prot. n. 7950/Gab;
VISTO il Decreto del Presidente della Regione n. 524/Serv.1°/SG, con il quale l'Avv. Giuseppa Mistretta, funzionario avvocato della Regione Siciliana, è nominato Commissario Straordinario dell'Istituto Regionale del Vino e dell'Olio, con i poteri di Presidente e del Consiglio di amministrazione fino all'insediamento degli organi ordinari di amministrazione;
VISTA la Delibera del C. S. n. 12 del 6/12/2024 con la quale viene approvato e sottoscritto il protocollo di intesa fra il Dipartimento regionale della Funzione pubblica e l'Istituto regionale del Vino e dell'Olio, avente ad oggetto l'assegnazione del Dott. Vito Bentivegna quale Direttore generale dell' IRVO;
VISTA la Delibera del C. S. n. 13 del 10/12/2024 con la quale il Dott. Vito Bentivegna, dirigente di terza fascia del Ruolo Unico della Regione Siciliana in assegnazione temporanea all'IRVO giusto DDG n. 5787 del 10 dicembre 2024, viene nominato Direttore generale dell'Istituto Regionale del Vino e dell'Olio, per la durata di anni tre, decorrenti dalla presa di servizio, nel rispetto della vigente disciplina;
CONSIDERATO che lo stesso ha preso servizio in data 10/12/2024, giusto protocollo 10741/2024;
VISTA la delibera del C.S. n. 14/2024 con la quale è stato approvato il relativo contratto individuale di lavoro;
VISTO il Regolamento Interno di Contabilità approvato con delibera commissariale n. 3 dell'11 settembre 2019 e approvato dalla Giunta di Governo con delibera n. 54 del 13 Febbraio 2020;
VISTA la delibera del Commissario Straordinario n. 16 del 27/12/2024 con la quale è stato approvato il bilancio di previsione triennale 2025-2027;

VISTA la nota 11418/2024 con la quale il predetto provvedimento è stato trasmesso all'Assessorato dell'Agricoltura, dello Sviluppo rurale e della Pesca;
VISTE le delibere commissariali 4/2025 e 13/2025 che apportano variazioni al predetto bilancio;
VISTO il Piano Triennale per l'Informatica nella PA 2024-2026, che inserisce una specifica Linea di azione (RA 3.3.1) che prevede l'obbligo per le PA di pubblicare entro il 30 giugno 2025, in "Amministrazione trasparente", il Manuale di Gestione Documentale;
DATO ATTO che il Manuale di Gestione Documentale è lo strumento che definisce il sistema di gestione dei documenti fornendo le istruzioni operative per il corretto funzionamento dei flussi e degli archivi, anche cartacei;
CONSIDERATO pertanto di dover adottare il documento, sentito l'incaricato per il supporto alla transizione digitale dell'IRVO, e di doverlo adottare con provvedimento formale, pubblicandolo nell'area "Amministrazione trasparente" - "Altri contenuti" - "Gestione documentale";
RITENUTO inoltre di doverne assicurare la massima diffusione all'interno dell'IRVO;
VISTE le indicazioni dettate in merito dal paragrafo 3.5 delle linee guida AGID sul "documento informatico"
VISTA lo schema di "Manuale di Gestione Documentale" dell'IRVO, versione 1.0, allegato al presente provvedimento;

DECRETA

per quanto espresso in premessa,
- Adottare il "Manuale di Gestione Documentale" dell'IRVO, versione 1.0, allegato e facente parte integrante del presente provvedimento;
- Pubblicare il manuale nell'area "Amministrazione trasparente" sez. "Altri contenuti" - "Gestione documentale";

Il presente decreto sarà pubblicato sul sito istituzionale ai sensi delle vigenti disposizioni in merito alla pubblicità ed alla trasparenza delle P.A.

_

Direttore Generale_
VITO BENTIVEGNA / ArubaPEC S.p.A._
(atto sottoscritto digitalmente)

documento firmato digitalmente da VITO BENTIVEGNA.
, 11/06/2025

REGIONE SICILIANA

ISTITUTO REGIONALE DEL VINO E DELL'OLIO

MANUALE DI GESTIONE DOCUMENTALE

versione 1.0 del …… DDG ……

Sommario

1. Scopo e campo di applicazione del documento

Obiettivo del presente Manuale di gestione - adottato ex art. 3 lett. d) del DPCM 3/12/2013 e secondo quanto previsto dal Piano Triennale per l'Informatica nella PA 2024/2026 (Linea di azione RA 3.3.1) - è descrivere il sistema di gestione documentale, a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita, e le funzionalità disponibili al personale abilitato all'utilizzo delle procedure.
Il Manuale è destinato alla più ampia diffusione interna, in quanto fornisce le istruzioni complete per la corretta gestione dei documenti da parte dei responsabili e degli addetti alle attività di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti nell'IRVO.

2. Aree Organizzative Omogenee e tenuta del protocollo informatico

L'amministrazione è costituita da un'unica Area Organizzativa Omogenea (AOO) denominata IRVO, composta dai seguenti uffici:

- Area Tecnica
- Direzione
- OdCC Olio
- OdCC Vino
- Presidente e CdA
- U.O. Contabilità
- U.O. Fiere
- U.O. Lab
- U.O. Microbiologia
- U.O. Osservatorio Vitivinicolo e Olivicolo oleario Regionale
- U.O. Ricerca Sperimentazione
- U.O. Risorse Umane
- U.O. Segreteria Organi Istituzionali
- U.O. Ufficio di Direzione

A queste si aggiungono le seguenti funzioni individuate con specifici provvedimenti per l'assegnazione dei documenti di specifica competenza:

- Responsabile Prevenzione Corruzione e Trasparenza
- Responsabile Servizio Prevenzione e Protezione
- Uff_eFatturaPA (UFI2ET)
- Ufficio Procedimenti Disciplinari

All'interno dell'AOO il sistema di gestione documentale e protocollazione è unico ed è totalmente decentrato (sia per la corrispondenza in entrata che in uscita), al fine di consentite ad ogni ufficio di svolgere anche l'attività di registrazione di protocollo.
Il Direttore Generale dell'IRVO, ai sensi dell'art. 17 del Codice dell'Amministrazione Digitale (CAD), è il responsabile della Transizione Digitale e della Conservazione ed è coadiuvato dal dirigente responsabile dell'Ufficio di Direzione e da un responsabile tecnico per le interlocuzioni tra la struttura ed il gestore esterno della piattaforma informatica dedicata.

2.1. Casella di posta elettronica

L'AOO si è dotata di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo telematico della AOO e di tutti gli uffici che ad essa fanno riferimento:
direzione.irvos@messaggipec.it
Oltre alla predetta PEC sono previste PEC dedicate per la fatturazione elettronica e per specifiche attività, oltre le caselle di posta ordinaria; gli indirizzi sono pubblicati sul sito dell'IRVO nella sezione contatti: https://www.irvos.it/contatti/

3. Piano di sicurezza informatica dei flussi documentali

L'Amministrazione si avvale, per la gestione documentale e per il protocollo informatico, di una web application.
Alla data di adozione della versione 1.0 del presente manuale, il servizio utilizzato è SICRAWEB EVO, erogato da Maggioli s.r.l., fruibile attraverso il sito: https://istitutooliovino.sicraweb.maggioli.cloud/

Tutte le relative attività di backup dei dati sono garantite nell'ambito del rapporto contrattuale di gestione del servizio. In virtù del servizio erogato, la Maggioli è stata nominata Responsabile in outsourcing del trattamento dati, ai sensi dell'art. 29 del D.Lgs. 30 giugno 2003 n.196.
La protezione dall'esterno è garantita da Sicilia Digitale, società a totale partecipazione della regione Siciliana, che gestisce la Intranet Regionale RTRS.

3.1. Criteri e modalità di rilascio abilitazioni accesso

L'abilitazione degli utenti al sistema SICRAWEB viene effettuata dal gestore delle utenze (supervisor facente capo all'U.O. Ufficio di Direzione. Gli utenti accedono al sistema tramite le credenziali rilasciate dal supervisor e in base al profilo di autorizzazioni assegnato. Per i nuovi utenti, al momento del primo accesso, è richiesto il cambio immediato della password ricevuta.
Le password di Sicraweb e del dominio attualmente prevedono una scadenza semestrale (180 giorni).

3.2. Regole di accesso ai documenti

L'accesso ai documenti è regolato dal sistema di autorizzazioni (profilo di abilitazione degli utenti) e dai criteri di assegnazione degli utenti agli uffici. Ciascun utente, associato a uno o più uffici, può accedere solo ai documenti assegnati agli uffici di appartenenza. Gli utenti con profilo di amministratore sono autorizzati ad accedere a qualsiasi documento.

3.3. Assegnazioni

L'utente autorizzato alla ricezione di un documento in entrata, all'atto della registrazione assegna lo stesso al responsabile della struttura competente e/o allo specifico destinatario. L'assegnatario deve prendere in carico il documento per la successiva gestione.
Nel caso di assegnazione errata, il destinatario che riceve il documento provvede a segnalarlo attraverso la specifica funzione del sistema affinché il documento venga correttamente assegnato all'ufficio di pertinenza.

3.4. Protezione dati

Per quanto riguarda il rispetto delle norme per la protezione dei dati di cui al GDPR 2016/679, si fa riferimento alle disposizioni dettate in marito dal Direttore dell'IRVO con circolare 3661/2024 "Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei" allegata e facente parte integrante del presente documento (allegato 1).

4. Formazione dei documenti informatici

I documenti informatici prodotti dall'amministrazione vengono generati di norma in uno dei formati previsti dalle linee guida AgID secondo quanto previsto dall'art.71 del CAD. Qualora i documenti vengano acquisiti nell'ambito del sistema di gestione documentale in formato diverso, vengono preliminarmente convertiti in pdf. I documenti informatici sono ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata.
Il sistema Sicraweb fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale ed i collegati movimenti finanziari; consente il reperimento delle informazioni riguardanti i documenti registrati;

5. Classificazione e conservazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO. Essa è eseguita a partire dal Titolario di classificazione adottato dall'Istituto (allegato 2)
Le delibere degli Organi Istituzionali ed i decreti del direttore generale, le cui procedure di adozione sono interamente gestite all'interno della piattaforma informatica, sono pubblicati sul sito web istituzionale www.irvo.it, nella sezione "provvedimenti" di Amministrazione Trasparente.

Le procedure atte a garantire la sicurezza nella formazione dei documenti informatici, e dei documenti protocollati, con particolare riferimento alla loro immodificabilità e integrità sono illustrate nel ***manuale della conservazione*** predisposto e adottato dalla ditta Maggioli, consultabile al seguente link: https://assistenza.maggioli.it/conservazione-digitale-documentazione/ .
Per quanto riguarda i tempi di conservazione si fa riferimento al "Piano di conservazione e scarto"

6. Flusso di lavorazione dei documenti ricevuti

Le fasi della gestione dei documenti ricevuti sono:
a) ricezione del documento;
b) assegnazione del documento agli uffici di pertinenza;
c) classificazione del documento associandolo ad una voce di Titolario;
d) registrazione e segnatura di protocollo.

7. Flusso di lavorazione dei documenti in uscita

Le fasi della gestione dei documenti spediti sono:
a) produzione del documento;
b) firma del responsabile;
c) classificazione del documento associandolo ad una voce di Titolario;
d) registrazione e segnatura di protocollo;
e) spedizione del documento.

8. Registrazione di protocollo

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:
a) il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) il mittente/destinatario del documento, registrato in forma non modificabile;
d) l'oggetto del documento, registrato in forma non modificabile.
e) il numero degli allegati
La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.
Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo si effettua per tutti i file allegati al documento.

8.1. Segnatura di protocollo

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
La segnatura è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
Essa consente di individuare ciascun documento in modo inequivocabile.
Le informazioni minime apposte od associate al documento mediante l'operazione di segnatura sono quelle elencate nelle linee guida AgID, e precisamente:
a) identificativo dell'Amministrazione;
b) tipo di corrispondenza (entrata/uscita);
c) numero e data protocollo
d) eventuale firma digitale del documento

8.2. Documenti esclusi dalla registrazione di protocollo

I documenti esclusi dal protocollo sono i seguenti:

- Gazzette e bollettini ufficiali
- materiale pubblicitario
- pubblicazioni e riviste varie
- atti preparatori interni

- generici inviti a manifestazioni

8.3.Documenti soggetti ad accesso riservato

Le procedure di registrazione a protocollo, adottate per la gestione dei documenti ad accesso riservato sono le stesse adottate per gli altri documenti e procedimenti amministrativi, con in più la compilazione della relativa scheda 4.
L'accesso ai documenti definiti al sistema come "riservati" è consentito esclusivamente agli utenti autorizzati e agli amministratori del sistema.

8.4. Annullamento delle registrazioni di protocollo

L'annullamento di una delle informazioni assegnate in automatico dal sistema e registrate in forma immodificabile determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo. In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale da consentire la lettura di tutte le informazioni originarie.
Il Direttore Generale ed il dirigente dell'Ufficio di Direzione sono i soli autorizzati a disporre o eseguire operazioni di annullamento/rettifica. Il sistema registra l'avvenuto annullamento/rettifica, la data e il soggetto che è intervenuto.

8.5. Registro giornaliero di protocollo

Il sistema permetta la stampa del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.
Il contenuto del registro giornaliero di protocollo è riversato automaticamente dall'applicativo, entro la giornata lavorativa successiva, nel sistema di conservazione.

8.6. Gestione delle emergenze

Il personale addetto alla gestione documentale deve assicurare, in caso di interruzione del servizio di protocollo, lo svolgimento delle operazioni di protocollazione su apposito registro di emergenza. Le informazioni relative ai documenti protocollati attraverso il registro di emergenza, vengono reinserite nel sistema informatico, al ripristino dello stesso, utilizzando un'apposita funzione di registrazione dei protocolli di emergenza.

9. Gestione fascicoli

Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o cartelle. Ogni documento, dopo la sua classificazione, deve essere inserito, a cura della struttura competente nel fascicolo di riferimento. Ogni struttura si fa carico di gestire i fascicoli e le pratiche di propria competenza, in formato digitale o cartaceo.

L'utente della struttura competente stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se esso si colloca nell'ambito di un procedimento amministrativo già aperto oppure se dà avvio ad uno nuovo:
1. Qualora un documento si collochi nell'ambito di un affare o procedimento in corso:
- si individua, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, quale sia il fascicolo relativo
- si seleziona il relativo fascicolo e si collega il documento al fascicolo selezionato;
- se si tratta di un documento su supporto cartaceo, si assicura l'inserimento fisico dello stesso nel relativo carteggio;
2. Se si dà avvio ad un nuovo fascicolo, la formazione di un nuovo fascicolo informatico avviene attraverso l'operazione di "creazione" che comprende la registrazione delle informazioni previste come essenziali dal sistema:
- si esegue quindi l'operazione di apertura del fascicolo;
- si collega il documento al nuovo fascicolo aperto.

Un documento, al momento della protocollazione, può essere inserito in più fascicoli mediante utilizzo del pulsante + in fascicoli/dettaglio.
Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferirà alla data dell'ultimo documento prodotto.

Quando si verifica un errore nell'assegnazione di un fascicolo, l'amministratore del sistema provvede a correggere le informazioni inserite nel sistema informatico e ad assegnare il fascicolo all'ufficio di competenza.

10. Conservazione dei documenti cartacei

La produzione di documenti cartacei riguarda prevalentemente atti istruttori o preparatori, essendo ormai il documento amministrativo digitale di default secondo quanto previsto dal Codice dell'Amministrazione Digitale (CAD).
l'IRVO conserva i fascicoli analogici negli armadi presenti in ciascuna delle strutture nelle quali è articolato, sotto la custodia dei responsabili dei diversi procedimenti.
Presso la sede di Palermo dell'Istituto è presente un archivio di deposito per la conservazione del materiale ivi depositato dalle diverse strutture in base alle richieste dei dirigenti competenti.
Per quanto riguarda i tempi di conservazione si fa riferimento al "Piano di conservazione e scarto".

11. Amministrazione Trasparente

In adempimento alla vigente normativa in tema di trasparenza e accesso civico (Decreto legislativo n. 33 del 14 marzo 2013 e successive modifiche − Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni), l'IRVO ha costituito apposita sezione di "Amministrazione trasparente" nel sito istituzionale www.irvo.it nella quale sono pubblicati dati, informazioni e documenti che riguardano l'organizzazione e le attività dell'amministrazione. Attraverso apposita sottosezione di Amministrazione trasparente è possibile consultare l'elenco dei "provvedimenti" amministrativi mediante diverse funzionalità di ricerca.

12. Norma transitoria

Per l'adozione del "Piano di conservazione e scarto", che integrerà il presente "manuale", dovrà essere effettuata una preventiva ricognizione degli obblighi da parte di ciascuna delle diverse strutture dell'IRVO, per ogni tipologia di procedura.
Nelle more, i documenti digitali e cartacei sono conservati in modo permanente ovvero per un determinato periodo di anni, in base a quanto previsto dalle normative vigenti applicabili a ciascuna tipologia di procedura dal CAD, dalle Linee guida AgID e dal Codice civile.

13. Norma di rinvio - pubblicazione

Per quanto non previsto dal presente documento si fa riferimento alle norme che regolano la produzione e la gestione dei documenti della P.A. dettate dal Codice dell'Amministrazione Digitale e dal DPR 445/2000.

Il presente manuale, come prescritto dall'art. 5 comma 3 delle Regole tecniche per il protocollo informatico, è pubblicato sul sito istituzionale dell'IRVO al fine di garantire la diffusione anche esterna all'Ente.

14. Allegati

1 - Circolare 3661/2024 "Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei"
2 - Titolario

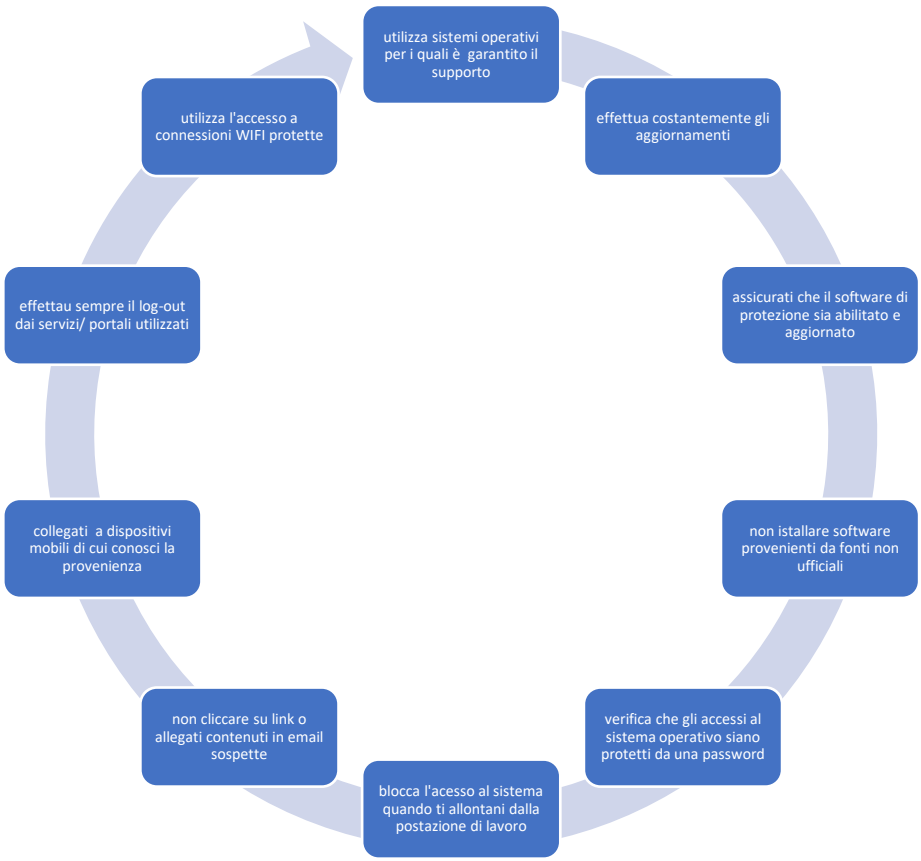
Palermo

Il Direttore Generale
dr V. Bentivegna

, 11/06/2025

Regole di condotta ed obblighi dei collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica redatto anche ai sensi del "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (da ora in poi GDPR) e del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007)

Rev.	Data	Motivo Revisione	Emissione: Titolare del Trattamento
00	25/02/2024	Prima Emissione	Istituto Regionale del Vino e dell'Olio



Indice del documento:

1. Riferimenti e definizioni

Reg. UE 2016/679 - GDPR: REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Provvedimenti del Garante della protezione dei dati personali:

- Deliberazione 23 novembre 2006 (G.U. 7 dicembre 2006, n. 285) "Linee Guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati."
- Deliberazione n. 13 del 1/3/2007 – (GU n° 58 del 10 marzo 2007) "Linee guida del Garante per posta elettronica e internet"
- Provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".
- Provvedimento n. 547 del 22 dicembre 2016 "Accesso alla posta elettronica dei dipendenti".

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Dispositivi aziendali: computer, portatili, smart phone, palmari, o qualsiasi altro strumento informatico di proprietà di Istituto Regionale del Vino e dell'Olio o comunque in uso per lo svolgimento delle attività lavorative.

Dipendente: personale assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Autorizzato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati personali riferiti a Istituto Regionale del Vino e dell'Olio.

2. Premessa

Durante l'attività lavorativa, i dipendenti e collaboratori di Istituto Regionale del Vino e dell'Olio, si ritrovano a gestire una serie di "**informazioni**", proprie e di terzi, per poter espletare la loro mansione.

Tali informazioni possono essere considerate, ai sensi del Reg. UE 2016/679 "**dati personali**" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che Istituto Regionale del Vino e dell'Olio adotti una serie di misure tecniche ed organizzative adeguate.

Altre informazioni, pur non essendo "dati personali", ai sensi di legge, sono in tutto e per tutto "**informazioni riservate**", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza, per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "**dati**" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, Istituto Regionale del Vino e dell'Olio tratta "**dati cartacei**" ovvero informazioni su supporto cartaceo e "**dati digitali**" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita di Istituto Regionale del Vino e dell'Olio.
Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, Istituto Regionale del Vino e dell'Olio ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare Interno si applica agli **Autorizzati** (*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare* ex art. 4 GDPR) che si trovino a trattare dati di qualsiasi natura, sia che abbiano ricevuto in consegna un dispositivo aziendale, sia che effettuino trattamenti esclusivamente cartacei o con strumenti informatici non ad uso esclusivo.
Una gestione dei dati cartacei, un uso dei COMPUTER e di altri dispositivi elettronici (di seguito DISPOSITIVI) nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate, nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.
Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell'art. 13 del Reg. UE 2016/679 e costituiscono, quindi, parte integrante dell'informativa rilasciata agli Autorizzati.

3. Autorizzazione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, Istituto Regionale del Vino e dell'Olio valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, di internet e della posta elettronica da parte degli Autorizzati. Successivamente e periodicamente l'azienda valuta la permanenza di tali presupposti.
E' fatto esplicito divieto, ai soggetti non autorizzati, di accedere agli strumenti informatici aziendali.

Hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli Autorizzati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.
Si sottolinea che le limitazioni alle autorizzazioni sono attuate in azienda, anche alla luce del Provvedimento del Garante 1/03/07 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

4. Titolarità dei dispositivi e dei dati

Istituto Regionale del Vino e dell'Olio è esclusiva titolare e proprietaria dei dispositivi messi a disposizione degli Autorizzati, ai soli fini dell'attività lavorativa; è, inoltre, l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.
L'incaricato non può ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i

files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

5. Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell'autorizzato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.
Qualsiasi eventuale tolleranza da parte di questa azienda, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

6. Restituzione dei dispositivi e dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'autorizzato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio di Istituto Regionale del Vino e dell'Olio, della permanenza dei presupposti per l'utilizzo dei dispositivi e dei dati cartacei aziendali, gli Autorizzati hanno i seguenti obblighi:
1. Procedere immediatamente alla restituzione dei dispositivi in uso;
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.
3. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
4. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati.

7. Le Password

Le password sono un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.
La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e a Istituto Regionale del Vino e dell'Olio nel suo complesso.
Istituto Regionale del Vino e dell'Olio ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Autorizzati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio, è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato, secondo il livello di sicurezza richiesto dall'azienda stessa e, comunque, in linea con quanto richiesto dalla normativa privacy.
Buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone.
Le password che non vengono utilizzate da parte degli Autorizzati per un periodo superiore ai sei mesi verranno disattivate da Istituto Regionale del Vino e dell'Olio.
In qualsiasi momento l'organizzazione si riserva il diritto di revocare al lavoratore il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

8. Regole per la corretta gestione delle password

A ciascun incaricato è affidato l'utilizzo e l'accesso ad un PC Client dotato di un sistema di autenticazione informatica, sistema che costituisce una delle regole tecniche a tutela dei dati di grande importanza.
In particolare, è previsto l'utilizzo da parte degli Autorizzati di apposite credenziali che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
Ciascun Incaricato è reso edotto del fatto che le credenziali di autenticazione sono personali:

- devono essere memorizzate;
- non devono essere comunicate a nessuno;
- non devono essere trascritte.

Le "credenziali di autenticazione" consistono in un codice per l'identificazione dell'Autorizzato ("user id") non assegnabile, neppure successivamente nel tempo, ad altro soggetto.
La credenziale di autenticazione deve essere associata a una parola chiave riservata conosciuta solamente dal medesimo ("password"), composta da almeno 8 (otto) caratteri, non contenente riferimenti agevolmente riconducibili all'utilizzatore.
La password, in particolare, deve rispettare i seguenti criteri:

• non deve contenere nomi comuni; • non deve contenere nomi di persona; • non deve essere riconducibile all'incaricato del trattamento; • non deve essere uguale alla user-id;	• deve contenere sia lettere che numeri; • deve comprendere caratteri alfabetici; • deve comprendere caratteri numerici e caratteri speciali; • non deve essere uguale alle precedenti; • deve essere lunga 8 caratteri od al numero massimo consentito dal sistema di autenticazione.

Agli Autorizzati è prescritta la modifica della password almeno ogni sei mesi. Agli Autorizzati è prescritto di adottare le necessarie cautele per assicurare la segretezza della password.
L'autenticazione dell'incaricato avviene tramite la verifica della "password" relativa alla "user-id" associata.
È previsto un sistema di "**password lock-out**" che blocca la procedura di accesso al Personal Computer, in seguito al verificarsi di un determinato numero di accesso falliti.
Tutti tentativi di accesso non autorizzati sono registrati.
L'amministratore di sistema provvede, ogni sei mesi, alla pulizia degli account per la disattivazione delle credenziali inutilizzate nel periodo, o riferite ad Autorizzati che hanno perso le qualità per accedere ai dati personali.

In caso di smarrimento della password l'utente deve tempestivamente richiedere una nuova procedura di assegnazione all'amministratore di sistema.

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:
1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili);
7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

9. Login e Logout

Il "Login" è l'operazione con la quale l'Autorizzato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro.
In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.
In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, Istituto Regionale del Vino e dell'Olio potrà assegnare un univoco user name e password per gruppi di Autorizzati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.
Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.
Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla, tale blocco sarà attivato automaticamente a seguito di un tempo predeterminato di mancato utilizzo.

10. Obblighi relativi all'uso dei dispositivi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.
L'incaricato deve quindi eseguire le operazioni seguenti:
1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo dispositivo, affinché persone non autorizzate non abbiano accesso ai dati protetti;
2. Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnere il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

11. Modalità d'uso del PC aziendale

Il sistema informativo aziendale utilizza gestisce i dati prevalentemente in cloud.
È obbligatorio il salvataggio, a fine giornata, dei dati processati su supporto ritenuto idoneo dal Titolare al fine di garantirne la sicurezza e il numero minimo di backup; Istituto Regionale del Vino e dell'Olio non effettua il backup dei dati memorizzati in locale.
Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema, utilizzando il proprio utente e password con privilegi di amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

In particolare l'Autorizzato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete della Istituto Regionale del Vino e dell'Olio ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
3. Mantenere sul computer esclusivamente i dispositivi approvati dall'organizzazione (memorizzazione, comunicazione, altro…);
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano Autorizzati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

Divieti Espressi sull'utilizzo del PC

All'Autorizzato è vietato:
1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta di Istituto Regionale del Vino e dell'Olio.
4. Installare alcun software di cui Istituto Regionale del Vino e dell'Olio non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare periferiche, dispositivi hardware e software (ad esempio hard disk, cam, telecamere, macchine fotografiche, smartphone, driver, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'organizzazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horse ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

12. Antivirus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- evitare lo scambio fra computer di supporti rimovibili (cd, dvd, zip) contenenti file con estensione .EXE, .COM, .OVR, .OVL, .SYS, .DOC , .XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non.

- disattivare la creazione di nuove finestre da parte del browser ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta, al fine di proteggersi dal codice HTML di certi messaggi e-mail (buona norma e visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso e in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare, immediatamente, l'Amministratore di Sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso e possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge.

Nel caso dl sistemi danneggiati seriamente da virus l'Amministratore di Sistema procede a reinstallare il sistema operativo, i programmi applicativi ed i dati.

13. Internet è uno strumento di lavoro

La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.
In particolare si vieta l'utilizzo dei social network, se non espressamente autorizzati, quale strumento di lavoro per es. di promozione dell'immagine aziendale.

L'organizzazione usufruisce del servizio di connettività fornito da Sicilia Digitale che stabilisce ed adotta idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.
Divieti Espressi concernenti Internet:
1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare categorie particolari di dati (dati sensibili) ai sensi del Reg. UE 2016/679.
2. È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all'Autorizzato lo scarico di software (anche gratuito) prelevato da siti Internet.

4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.
5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
6. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.
7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
8. È vietato all'Autorizzato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
9. E' vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dal fornitore Sicilia Digitale e lo strumento VPN messo a disposizione.
10. È vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su Internet, a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
11. È vietato accedere a siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati da Istituto Regionale del Vino e dell'Olio e gestiti da Sicilia Digitale per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.
12. È vietato utilizzare l'accesso ad internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6/05/99, n. 169 e legge 18/08/00, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dall'organizzazione.
Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali, è posta sotto la personale responsabilità dell'Incaricato inadempiente.

14. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali non è ammesso.
Gli Autorizzati possono avere in utilizzo indirizzi nominativi di posta elettronica. Tale account è pur sempre riservato, ma in tali casi la personalità (nome e cognome riportato) dell'indirizzo non significa che si tratti di un indirizzo privato.
Pertanto, non appare, astrattamente, prospettabile un suo diritto all'utilizzo esclusivo e riservato di una casella di posta elettronica aziendale. Talvolta, infatti, potrà essere necessario l'accesso e la lettura da parte di soggetti diversi, sempre appartenenti alla azienda, rispetto al suo consuetudinario utilizzatore, al fine, per esempio, di effettuare la manutenzione delle caselle di posta o di consentire la regolare continuità dell'attività di Istituto Regionale del Vino e dell'Olio, nelle ipotesi di sostituzioni di colleghi per ferie, malattia, etc...
Gli Autorizzati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, …,) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

Gli Autorizzati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Autorizzati e allo scopo prevede le seguenti misure:
1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio, al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

15. Divieti Espressi nell'uso della posta elettronica

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.
2. È opportuno redigere i messaggi di posta elettronica diretti a destinatari esterni dell'organizzazione, tramite l'indirizzo aziendale, utilizzando sempre la formula di disclaimer trasmessa dall'azienda.
3. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria e comunque, con gli indirizzi in chiaro di tutti i destinatari.
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
7. È opportuno limitare l'utilizzo della posta elettronica per messaggi con allegati di grandi dimensioni.

Ed inoltre, si sottolinea:
1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

16. Posta Elettronica in caso di assenze programmate, non programmate.

Nel caso di assenza prolungata sarà buona norma attivare il servizio di risposta automatica (Auto-reply).
A tal fine, è cura dell'amministratore di sistema, mettere a disposizione dell'incaricato anche apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente in caso di assenze (per es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto dell'incaricato assente o della Istituto Regionale del Vino e dell'Olio.

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail, per ragioni di operatività aziendale, l'Autorizzato deve nominare un collega fiduciario con comunicazione scritta che, in caso di assenza, inoltri i files necessari a chi ne abbia urgenza.
Qualora l'Autorizzato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, Istituto Regionale del Vino e dell'Olio, informerà preventivamente (e solo ove non sia possibile successivamente) il lavoratore stesso, spiegando modalità e motivazioni dell'intervento, che il contenuto dei messaggi di posta elettronica verrà verificato da un incaricato, temporaneamente, modificando le credenziali di accesso. Di tale attività sarà redatto apposito verbale.

L'eventuale controllo o il monitoraggio delle mail sarà sempre graduale, dovendosi così escludere l'ammissibilità di controlli prolungati, costanti o indiscriminati; sono comunque vietate la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.
Ogni forma di controllo occulto è vietata e comunque in Istituto Regionale del Vino e dell'Olio è vietato l'uso di "sniffer" o altri dispositivi hardware o software finalizzati all'intercettazione e/o all'interruzione e/o all'impedimento di comunicazioni telematiche, come quelle che avvengono tramite e-mail.

17. Posta Elettronica in caso di cessazione dell'incarico

In caso di cessazione per qualsivoglia ragione e/o causa del rapporto di lavoro e/o di collaborazione e/o altro in essere con Istituto Regionale del Vino e dell'Olio, gli account riconducibili a persone identificate o identificabili saranno rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi, riferiti all'attività professionale del titolare del trattamento. (*L'interesse di Istituto Regionale del Vino e dell'Olio ad accedere alle informazioni necessarie all'efficiente gestione della propria attività, pertanto, verrà contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi*).
Le email precedentemente archiviate nell'account del dipendente cessato non potranno essere custodite, all'interno del server, per un periodo di tempo superiore a 3 mesi "fatta salva la conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria".

18. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "dispositivo mobile") possono venire concessi in uso dall'organizzazione agli Autorizzati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.
L'Autorizzato è responsabile dei dispositivi mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai dispositivi mobili si applicano le regole di utilizzo previste per i PC, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui dispositivi mobili devono essere trasferiti sulle memorie di massa aziendali, al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili.
Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dalla direzione.
I dispositivi mobili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo protetto.
Anche di giorno, durante l'orario di lavoro, all'Autorizzato non è consentito lasciare incustoditi i dispositivi mobili.
E' vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto o in albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.
Laddove il dispositivo mobile sia accompagnato da un'utenza, l'Autorizzato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'esterno devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

19. Memorie esterne (chiavi usb, hard disk, memory card, ecc.)

Agli Autorizzati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).
Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

20. Dispositivi personali

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali.
In tal caso è necessario che il dispositivo abbia password di sicurezza stringenti approvate dalla direzione.
Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, DVD, macchine fotografiche, videocamere, tablet, …).
Gli Autorizzati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri dispositivi personali per memorizzare dati di Istituto Regionale del Vino e dell'Olio, solo se espressamente autorizzati dalla direzione e assumendone formalmente e personalmente l'intera responsabilità del trattamento.
Tali dispositivi dovranno essere preventivamente valutati dall'amministratore di sistema, per la verifica della sussistenza delle idonee misure tecniche di sicurezza.

21. Distruzione dei Dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli Autorizzati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, ecc.), al termine del loro utilizzo dovranno essere restituiti a Istituto Regionale del Vino e dell'Olio che provvederà a distruggerli o a ricondizionarli nel modo più idoneo.
In particolare Istituto Regionale del Vino e dell'Olio provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

22. Utilizzo del cellulare/smartphone personale.

Durante l'orario di lavoro, comprese le eventuali pause, agli Autorizzati è concesso l'utilizzo del telefono cellulare personale, ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo. In caso di trasferte lavorative all'esterno degli uffici dell'organizzazione, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'organizzazione stessa ove fosse necessario.

23. Utilizzo delle stampanti

L'incaricato deve effettuare la stampa dei dati solo se necessaria all'attività lavorativa e deve ritirarla prontamente dai vassoi delle stampanti personali/comuni per evitare che sia visibile o possa essere

raccolta da terzi. Al momento del ritiro dei fogli stampati, l'utente deve porre attenzione a prelevare solo le proprie pagine.
L'incaricato, qualora disponga di più dispositivi di stampa, deve utilizzare quello che garantisce un maggior controllo del documento stampato.

24. Utilizzo di sistemi cloud

È vietato agli incaricati l'utilizzo di sistemi Cloud non espressamente approvati dall'Azienda. Per essere approvati i sistemi cloud devono rispondere ai requisiti di sicurezza.

25. Smart Working, Telelavoro, lavoro in trasferta.

Per determinate situazioni di emergenza o per accordi con i lavoratori, questa Azienda può permettere ad alcuni lavoratori di svolgere la loro attività da remoto, dalla propria abitazione o mentre si trova in trasferta.
In tali situazioni, l'Incaricato dovrà verificare:
1) Di disporre di una connessione internet sicura, attraverso una verifica delle wi-fi casalinga o optando per una connessione mobile protetta.
2) Svolgere la propria attività verificando che non sia possibile per terzi, anche famigliari, accedere o anche solo visionare quanto si stia facendo.
3) attivare la sospensione automatica del dispositivo in uso, al fine di evitare accessi non controllati.

26. Organizzazione della scrivania

Gli Autorizzati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Gli Autorizzati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede agli Autorizzati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione da Istituto Regionale del Vino e dell'Olio.
I principali benefici di una politica della scrivania pulita sono:
1) Una buona impressione a clienti e fornitori che visitano la nostra Istituto Regionale del Vino e dell'Olio;
2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
3) La riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Autorizzati riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti in sede.
A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.
Ove possibile, si invita ad evitare la stampa di documenti digitali.
Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.
Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

27. In caso di furto

In caso di perdita o furto dei dispositivi consegnati e/o di documentazione aziendale, sarà obbligo dell'incaricato comunicare via mail a direzione.vitevino@regione.sicilia.it tempestivamente, al momento

della scoperta, l'accaduto, circostanziando il fatto dettagliatamente, in modo che l'azienda possa procedere con le denunce del caso e l'attuazione delle contromisure ritenute opportune.

28. Controlli

Istituto Regionale del Vino e dell'Olio, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.
Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

29. Modalità di verifica

Istituto Regionale del Vino e dell'Olio promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Autorizzati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.
Istituto Regionale del Vino e dell'Olio informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Autorizzati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.
Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.):

- si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite;
- si procederà ad effettuare controlli più mirati che coinvolgano i dipendenti afferenti all'area o al settore in cui è stata rilevata l'anomalia.

30. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

1. Ad esigenze tecniche o di sicurezza del tutto particolari;
2. All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

31. Segreto aziendale

Il dipendente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dalla Società, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.

Gli obblighi del dipendente previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

32. Individuazione dei Soggetti autorizzati

Istituto Regionale del Vino e dell'Olio ha designato un amministratore di sistema cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.
Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, gli Autorizzati della manutenzione) sono stati appositamente Autorizzati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.
I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

33. Cosa fare in caso di violazione dei dati personali?

Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati si configura come un **data breach**. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
    - invio per errore di e-mail contenenti dati personali a destinatari scorretti (mail che viene inviata per errore ad un altro destinatario rispetto a quello previsto)
    - invio per errore di e-mail con molteplici indirizzi in chiaro (indirizzi in a o in cc)
- il furto o la perdita di dispositivi informatici contenenti dati personali; (furto di PC, di telefonini aziendali, ecc..)
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Qualora nell'espletamento delle Vs funzioni doveste riscontrare una delle ipotesi su elencate, sarà Vs compito comunicarlo al Vs superiore gerarchico, con assoluta tempestività, in modo tale che l'Ente possa immediatamente attivarsi, entro le 72ore di tempo limite, nell'attuazione di quanto disposto dal GDPR. Tale comunicazione deve costituire una priorità assoluta, nel rispetto di quanto indicato *05_01_Istruzioni_Operative_Data_Breach*

34. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle condotte, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. Il biasimo inflitto verbalmente;
2. Lettera di richiamo inflitto per iscritto;
3. Sanzione disciplinare;
4. La sospensione dalla retribuzione e dal servizio;
5. Il licenziamento disciplinare.

35. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere ai sensi del Capo III del GDPR alle informazioni che lo riguardano scrivendo all'indirizzo mail direzione.vitevino@regione.sicilia.it

36. Validità, aggiornamento e diffusione

Il presente Disciplinare ha validità a partire da: _____(data)

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative. Ogni variazione del presente Disciplinare sarà comunicata agli Autorizzati.
Il presente Disciplinare verrà pubblicato sul sito internet dell'Istituto nella sezione "regolamenti" https://www.irvos.it/atti-amministrativi-generaliregolamenti/ ai sensi dell'art. 7 della legge 300/70 e del CCNL.

Data _____

Firma del Titolare del trattamento dei dati
Istituto Regionale del Vino e dell'Olio

REGIONE SICILIANA

ISTITUTO REGIONALE DEL VINO E DELL'OLIO

Allegato 2 al Manuale di Gestione Documentale

Titolario di classificazione dei documenti

Il Titolario di Classificazione è lo schema logico di organizzazione funzionale dei documenti dell'IRVO. Esso va obbligatoriamente utilizzato fin dalla fase di adozione di delibere, decreti del direttore generale e registrazione di protocollo.
Per ogni modifica del presente Titolario di classificazione, vanno informati tutti i soggetti abilitati all'operazione di classificazione dei documenti.

Il Titolario si riferisce alla documentazione prodotta/ricevuta da tutte le strutture dell'IRVO. Esso si suddivide in titoli, i quali si suddividono in classi, che permettono la costruzione dei fascicoli. Il Titolario si basa sulle funzioni dell'ente, quindi è del tutto indipendente dai modelli organizzativi e dagli organigrammi dell'ente.
La logica che guida la classificazione dei singoli documenti è quella del procedimento a cui è collegato il documento/atto che si protocolla. Ogni documento, dopo la sua classificazione, va inserito nel fascicolo a cura della struttura competente.
Il fascicolo, quale unità archivistica, è un insieme ordinato di documenti riferito in modo stabile ad uno stesso processo amministrativo, ad una stessa materia, ad una stessa tipologia, e può coincidere con un procedimento amministrativo o parte di esso o più procedimenti amministrativi. I documenti si conservano all'interno di ciascun fascicolo o sotto fascicolo, secondo l'ordine cronologico di registrazione.

Il Titolario dell'IRVO ha 2 livelli o voci: titolo, classe. Ogni voce è identificata attraverso un codice composto da numeri; la combinazione dei numeri delle diverse voci, secondo il suddetto schema, costituisce l'"Indice di classificazione", cioè il codice identificativo che individua la posizione logica di ogni fascicolo all'interno del complesso documentario dell'Istituto. I numeri che compongono l'indice di classificazione, riferiti cioè a titolo e classe, (entrambe indicate con numeri arabi), sono separati tra loro attraverso un punto. Ad esempio, l'effettuazione di un concorso o di un bando di selezione del personale corrisponde a "titolo 3, classe 1".

L'indice di classificazione, combinato con l'identificativo del fascicolo, individua il posto preciso che ogni singolo documento andrà ad occupare all'interno dell'archivio informatico.

La posizione del singolo fascicolo all'interno dell'elenco dei fascicoli relativi ad ogni a classificazione è determinata dalla data di apertura dello stesso; l'identificativo del fascicolo è individuato con un numero ed un anno separati da una barra (esempio N.10/2025); l'eventuale sotto fascicolo è inserito dopo il numero del fascicolo, separato da un punto prima della barra (esempio N.10.1/2025).

Titoli classificazione adottati dall'IRVO

1 AMMINISTRAZIONE GENERALE

1.1 LEGISLAZIONE E CIRCOLARI ESPLICATIVE
1.2 PIANI E PROGRAMMI
1.3 STATUTO
1.4 REGOLAMENTI
1.5 CIRCOLARI E DIRETTIVE
1.6 SISTEMA PRIVACY
1.7 SISTEMA INFORMATIVO
1.8 INFORMAZIONI E RELAZIONI CON IL PUBBLICO
1.9 POLITICA DEL PERSONALE; ORDINAMENTO DEGLI UFFICI E DEI SERVIZI
1.10 RELAZIONI CON LE ORGANIZZAZIONI SINDACALI E DI RAPPRESENTANZA DEL PERSONALE
1.11 CONTROLLI INTERNI ED ESTERNI
1.12 EDITORIA E ATTIVITA' INFORMATIVO-PROMOZIONALE INTERNA ED ESTERNA
1.13 ADEMPIMENTI STATISTICI E RILEVAZIONI
1.14 ATTIVITÀ DI RAPPRESENTANZA E SPONSORIZZAZIONI
1.15 INCARICHI PROFESSIONALI
1.16 TRASPARENZA E ANTICORRUZIONE
1.17 SERVIZIO PREVENZIONE E PROTEZIONE

2 ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA

2.1 PRESIDENTE
2.2 CONSIGLIO DI AMMINISTRAZIONE
2.3 COMMISSARIO
2.4 COLLEGIO DEI REVISORI
2.5 DIRETTORE GENERALE
2.6 DIRIGENTI
2.7 OIV

3 RISORSE UMANE

3.1 CONCORSI, SELEZIONI, COLLOQUI
3.2 ASSUNZIONI E CESSAZIONI
3.3 PERSONALE NON DIPENDENTE; COMANDI E DISTACCHI; MOBILITA'
3.4 MISSIONI
3.5 INQUADRAMENTI E APPLICAZIONECONTRATTI COLLETTIVI DI LAVORO
3.6 RETRIBUZIONI E COMPENSI
3.7 TRATTAMENTO FISCALE, CONTRIBUTIVO ED ASSICURATIVO
3.8 TUTELA DELLA SALUTE E SICUREZZA SUL LUOGO DI LAVORO
3.9 DICHIARAZIONI DI INFERMITA' ED EQUO INDENNIZZO
3.10 INDENNITA' PREMIO DI SERVIZIO E TRATTAMENTO DI FINE RAPPORTO, QUIESCENZA
3.11 SERVIZI AL PERSONALE SU RICHIESTA
3.12 ORARIO DI LAVORO, PRESENZE E ASSENZE
3.13 GIUDIZI, RESPONSABILITA' E PROVVEDIMENTI DISCIPLINARI

3.14 FORMAZIONE E AGGIORNAMENTO PROFESSIONALE
3.15 OGGETTI DIVERSI
3.16 ORDINI DI SERVIZIO

4 RISORSE FINANZIARIE E PATRIMONIO

4.1 BILANCIO PREVENTIVO
4.2 GESTIONE DEL BILANCIO
4.3 GESTIONE DELLE ENTRATE: ACCERTAMENTO, RISCOSSIONE, VERSAMENTO
4.4 GESTIONE DELLA SPESA: IMPEGNO, LIQUIDAZIONE, ORDINAZIONE E PAGAMENTO
4.5 PARTECIPAZIONI FINANZIARIE
4.6 RENDICONTO DELLA GESTIONE, ADEMPIMENTI E VERIFICHE CONTABILI
4.7 ADEMPIMENTI FISCALI CONTRIBUTIVI ASSICURATIVI
4.8 BENI IMMOBILI
4.9 BENI MOBILI: GESTIONE INVENTARIALE
4.10 ECONOMATO
4.11 RAPPORTI CON LA REGIONE
4.12 TESORERIA
4.13 ACQUISTO BENI E SERVIZI; LAVORI

5 AFFARI LEGALI

5.1 CONTENZIOSO
5.2 RESPONSABILITA' CIVILE E PATRIMONIALE VERSO TERZI; ASSICURAZIONI
5.3 PARERI E CONSULENZE

6 ATTIVITA' ISTITUZIONALI

6.1 ODCC VINO
6.2 ODCC OLIO
6.3 LABORATORI
6.4 MANIFESTAZIONI FIERISTICHE E PROMOZIONALI
6.5 PROGETTI - PARTENARIATI – CONVENZIONI
6.6 RICERCA E SPERIMENTAZIONE
6.7 MICROBIOLOGIA
6.8 SERVIZI ALLE AZIENDE
6.9 FORMAZIONE
6.10 ALTRI SERVIZI
6.11 INNOVAZIONE
6.12 OSSERVATORIO

7 OGGETTI DIVERSI

7.1 OGGETTI DIVERSI