POLITIQUES ET PRATIQUES ENCADRANT LA GOUVERNANCE DES RENSEIGNEMENTS PERSONELS PAR CERBA RESEARCH CANADA

(Document à être publié sur le site Internet de Cerba Research)

A. Éléments constitutifs du programme de gouvernance		
Engagement organisationnel	**a) Participation de la direction**	La direction appuie le programme de gouvernance des renseignements personnels (RP) et promeut une culture respectueuse de la vie privée en faisant ce qui suit : • Nommer le responsable de la protection des RP (Responsable PRP); • Approuver les mesures de contrôle du programme; • Contrôler le programme et présenter des rapports au conseil d'administration, le cas échéant; • Fournir les ressources nécessaires pour assurer la réussite du programme.
	b) Responsable PRP	Responsable de l'élaboration et de la mise en œuvre des mesures de contrôle du programme et de leur évaluation et révision continue.
	c) Préparation de rapports	L'organisation a établi des mécanismes redditionnels et en tient compte dans les mesures de contrôle de son programme.
Mesures de contrôle du programme de gouvernance	**a) Inventaire des RP**	L'organisation est en mesure de déterminer : • Les RP qu'elle possède ou contrôle; • La nécessité de recueillir, d'utiliser et de communiquer des RP; • La nature sensible des RP; • Les mesures de sécurité en place.
	b) Politiques, directives et procédures	• Politique de protection des RP qui détaille les rôles et responsabilités des membres du personnel tout au long du cycle de vie de ces renseignements; • Directive sur la collecte, l'utilisation et la communication de RP; • Directive sur la conservation, la destruction et l'anonymisation de RP; • Directive sur les mesures de sécurité des RP; • Procédure de traitement des demandes et des plaintes relatives aux RP;

		• Procédure de gestion des incidents de confidentialité impliquant un RP; • Politique de confidentialité des RP recueillis via le site Internet.
	c) Outils d'évaluation du risque	Grille d'évaluation des facteurs relatifs à la vie privée (EFVP) pour : • Tout projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de RP; • Communiquer des RP à l'extérieur du Québec ou confier à un tiers situé à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte des RP; • Communiquer des RP à un tiers sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques. Grille d'évaluation du risque de préjudice sérieux en cas d'incident de confidentialité.
	d) Formation et sensibilisation	Un programme de formation qui vise l'ensemble des employés, incluant les cadres, et qui couvre notamment les sujets suivants : • Les lois, politiques-directives-procédures internes applicables en matière de protection des RP; • Des techniques afin d'identifier et de reconnaître les incidents de confidentialité; • Le traitement des plaintes et des demandes en matière de protection des RP; • Les conséquences de la violation des lois et des règles internes en matière de protection des RP.
	e) Protocole de gestion en cas d'incident de confidentialité	L'organisation a mis en place une procédure et nommé une personne responsable de la gestion des incidents de confidentialité qui concernent des RP. Elle a clairement défini les responsabilités en matière de déclarations internes et externes des violations. L'organisation tient un registre de tous les incidents de confidentialité, même ceux qui ne comportent pas de risque de préjudice sérieux.
	f) Gestion des fournisseurs de service	L'organisation incorpore des clauses de confidentialité ou conclut avec ses fournisseurs de service un contrat

		de sous-traitance des données qui prévoient notamment: • Les mesures de protection des RP; • L'utilisation des RP aux fins de l'exécution du contrat; • La destruction des RP à l'issue du contrat; • L'obligation pour le fournisseur de services de notifier sans délai l'organisation en cas de violation ou tentative de violation des obligations de confidentialité; • La possibilité pour l'organisation de demander tout document et d'effectuer toute vérification relative à la confidentialité des RP.
	g) Communication externe	L'organisation informe les personnes de leurs droits en matière de protection des RP et des mesures de contrôle de son programme de gouvernance. La politique de confidentialité disponible sur le site Internet de l'organisation est rédigée en termes simples et clairs et inclut notamment : • Les finalités de la collecte, de l'utilisation et de la communication des RP ainsi que leur protection et durée de rétention; • Informer les personnes si leurs RP sont communiqués à des tiers et à l'extérieur du Québec; • Les coordonnées du Responsable PRP à qui faire part des questions, des demandes ou des plaintes.
B. Évaluation et révision continues du programme de gouvernance		
Plan de surveillance et de révision	L'organisation a élaboré un plan de surveillance et de révision annuel qui établit comment elle surveille et évalue l'efficacité des mesures de contrôle de son programme de gouvernances des RP.	
Évaluer et réviser les mesures de contrôle du programme de gouvernance au besoin	1. Mettre à jour l'inventaire des RP; 2. Réviser les politiques, directives et procédures; 3. Traiter les outils d'évaluation du risque comme des documents à caractère évolutif; 4. Modifier les cours de formation et de sensibilisation; 5. Adapter le protocole de gestion en cas d'incident de confidentialité; 6. Peaufiner la gestion des fournisseurs de services; 7. Améliorer les communications externes.	