PRIVACY POLICY

MyHSA-POL-015

VERSION HISTORY

Version	Date of Change	Responsible for Change	Summary of Change
2.0	January 2021	myHSA, Mark Young, CTO	Alignment to ISO 27002 Best Practices and minor Content Changes
1.1	May 2019	myHSA, Mark Young, CTO	Review draft and updates specific to myHSA compliance to ISO 27001
1.0	January 2019	Scalar Decisions	First full draft

Associated documentation:	**Legal Framework:** Freedom of Information and Protection of Privacy Act, Personal Information Privacy Electronic Documents Act (PIPEDA), ISO 27002 Best Practices **Policies:** Information Security Policy, Acceptable Use Policy, Data Breach Response Policy, Access Control Policy
Appendices:	Appendix A - Definitions
Approved by:	Mark Young, CTO
Date:	February 1, 2023
Confidentiality level:	CONFIDENTIAL

Review and consultation process:	This process will be reviewed on an annual basis by IT and Management with review by Contego Inc. as required.

OWNERSHIP & APPROVAL

Policy Owner	Tim Kane, Chief Executive Officer
Policy Approver(s)	Mark Young, Chief Technology Officer
Last Review Date	February 1, 2023
Approval Date	February 1, 2023

When in printed form, this document is uncontrolled.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE

myHSA is committed to information security and privacy. In accordance with this commitment, MyHSA has developed and established an Information Security Management System (ISMS), for which a component of that system includes our Privacy Policy. Thus, the key objective of the Policy is to guide myHSA executives with directions on how to communicate our privacy policy to its employee's, partners, and clients.

2. SCOPE

This policy applies to all users which include but not limited to employees, partners, clients, contractors, part-time and temporary workers, trainees, service providers, and those employed by others to perform work at myHSA. myHSA is committed to providing safe computing and has implemented this Privacy Policy to demonstrate our firm commitment to our client's privacy. myHSA complies with Canadian Federal and Provincial privacy laws and regulations including the Personal Information Protection and Electronic Documents Act and the Personal Information Protections Act.

3. POLICY

3.1 GENERAL

- myHSA assumes full accountability for the personal information within its possession and control. This organization has appointed a Privacy Officer as custodian of all privacy matters and legal compliance with privacy laws.

- We obtain personal information directly from the individual to which the information belongs. Individuals are entitled to know how we use personal information and will limit the use of any personal information collected only to what is needed for those stated purposes.

- We will obtain individual consent if personal information is to be used for any other purpose. We will not use that information without the consent of the individual. Under no circumstances will we sell, distribute, or otherwise disclose personal information or contact lists to third parties. However, limited disclosure may be required as part of us fulfilling our stated business duties and day-to-day operations. This may include our consultants, suppliers, or business partners but only with the understanding that these parties obey and abide by this Privacy Policy, to the extent necessary of fulfilling their own business duties and day-to-day operations.

- We will retain personal information only for the duration it is needed for conducting business. Once personal information is no longer required, it will be destroyed in a safe and secure manner and according to our Data Retention and Destruction Policy. However, certain laws may require that certain personal information be kept for a specified amount of time. Where this is the case, the law will supersede this policy.

- We vow to protect personal information with the appropriate security measures, physical safeguards, and electronic precautions. As per our Data Breach Response Policy, we will notify all affected individuals of a security event or breach that pertains to their personal information.

- myHSA is a paperless environment so we maintain personal information through electronic files. Where required by law or disaster recovery/business continuity policies, older paper records may be stored in a secure, offsite location.

    - Access to personal information will be authorized only for the employees and agents who require the information to perform their job duties, and to those otherwise authorized by law.
    - Our computer and network systems are secured by complex passwords. Only authorized individuals may access secure systems and databases.
    - Routers and servers connected to the Internet are protected by a firewall and are further protected by virus attacks or "snooping" by sufficient software solutions.
    - Personal information is not transferred to volunteers, summer students, interns, or other non-paid staff by e-mail or any other electronic format

3.2 WEBSITE

- myHSA is committed to providing safe web sites for visitors of all ages and has implemented this Privacy Policy to demonstrate our firm commitment to your privacy. myHSA complies with Canadian Federal and Provincial privacy laws and regulations including the Personal Information Protection and Electronic Documents Act and the Personal Information Protections Act.

- We use your Personal Information only for providing and improving the Site. By using the Site, you agree to the collection and use of information in accordance with this policy.

- There may be links from our Site to other web sites; note that this Privacy Policy applies only to our Site and not to web sites of other companies or organizations to which our Sites may be linked. You must check on any linked sites for the privacy policy that applies to that site and/or make any necessary inquiries in respect of that privacy policy with the operator of the linked site. These links to third party websites are provided as a convenience and are for informational purposes only. The Company does not endorse, and is not responsible for, these linked websites.

3.2.1 Information Collection and Use

- While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personal Information is information about you that identifies you as an individual, for example, your name, address, e-mail address, or telephone number. ("Personal Information").

3.2.2 Log Data

- Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data"). This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics. In addition, we may use third party services such as Google Analytics that collect, monitor, and analyze this …

3.2.3 Communications

- We may use your Personal Information to contact you with information pertaining to your myHSA account(s).
- If user/client requires access to their personal information that we have on file, a request can be made to our Privacy Officer. Also, if user/client wishes myHSA to destroy or delete sections or their entire information, it will be done so based on myHSA's Data Retention and Destruction Policy. Your request for access, additions and/or deletions will be recorded and filed by myHSA.
- If myHSA requires more personal information that we currently have to successfully provide you proper service, we will communicate the information required via email. Response to that email will constitute consent.
- If you do not permit us to use your Personal Information, your access to our services may be denied. You can appeal this decision by sending an email to cchromiak@contegosecurity.com or writing to:

Privacy Officer
myHSA Inc.
2024 34 Ave SW
Calgary, AB T2T 2C3

- User/clients consents that it may take up to 10 business day in order for myHSA to respond to and Inquiries, Complaints and/or Disputes.

3.2.4 Cookies

- myHSA, in common with many web site operators, may use standard technology called "cookies" on its Sites. For security and confidential reasons, we do not use cookies to store any confidential information such as passwords. Cookies are small data files that are downloaded onto your computer when you visit a particular web site. You can disable cookies by turning them off in your browser: however, some areas of the Site may not function properly if you do so.

3.2.5 Security

- We have put in place physical, electronic, and managerial procedures to safeguard and help prevent unauthorized access, maintain data security, and correctly use the information we collect online. myHSA applies security safeguards appropriate to the sensitivity of the information, such as retaining information in secure facilities, encryption of sensitive data and making personal information accessible only to authorized employees on a need-to-know basis.

- The security of your Personal Information is important to us but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means such as SSL and encryption to protect your Personal Information, we cannot guarantee its absolute security.

3.2.6 Storage of Information

- Personal information you share with us is securely stored on our database servers at AWS data centers in Montreal, Canada.

3.2.7 Changes To This Privacy Policy

- This Privacy Policy has been in effective as of 01/01/2017 and will remain in effect except with respect to any changes in its provisions in the future, which will be in effect immediately after being posted on this page.
- We reserve the right to update or change our Privacy Policy at any time and you should check this Privacy Policy periodically. Your continued use of the Service after we post any modifications to the Privacy Policy on this page will constitute your acknowledgment of the modifications and your consent to abide and be bound by the modified Privacy Policy.
- If we make any material changes to this Privacy Policy, we will notify you either through the email address you have provided us, or by placing a prominent notice on our website.

4. ENFORCEMENT AND COMPLIANCE

Compliance with myHSA policies is mandatory and places the following responsibilities on myHSA members with access to myHSA's information assets:

- Information Security Officers will ensure that myHSA management understand and follow this policy and conduct periodic reviews to ensure compliance.
- It is the responsibility of all myHSA management to ensure their areas of responsibility comply with this policy.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Audits will be performed on a yearly basis by our authorized 3rd Party vendor.

Audits will be managed by IT, in accordance with the Risk Management Policy. IT will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification. Every effort will be made to prevent audits from causing operational failures or disruptions.

This policy is compliant to the ISO 27002 Best Practices

5. ACKNOWLEDGEMENT AND AGREEMENT

I acknowledge that I have read and understand the Privacy Policy. I agree to adhere to this policy and will ensure that employees working under my direction adhere to this policy. I understand that if I violate the rules set forth by this policy, I may face disciplinary action up to and including termination of employment.

Name: _____

Signature: _____

Date: _____

Witness: _____

6. APPENDIX A - DEFINITIONS

- **Privacy Officer** Chris Chromiak, CISO, cchromiak@contegosecurity.com - The first point of contact within myHSA when **privacy** issues arise. Chris Chromiak has the authority to intervene on **privacy** issues relating to any of myHSA's operations.

- **Personally, Identifiable Information** - Any identifying information about an individual or group of individuals, including name, date of birth, address, phone number, e-mail address, social insurance/security number, nationality, gender, health history, financial data, credit card numbers, bank account numbers, assets, debts, liabilities, payment records, credit records, loan records, opinions, and personal views.

- **Business Information** - Our business address, business telephone number, name(s) of owner(s), executive officer(s), and director(s), job titles, business registration numbers, and financial status. Business information is treated and handled with the same level of confidentiality, privacy, and respect as personal information.