PROFOUND MEDICAL CORP.
CYBERSECURITY and
ELECTRONIC MONITORING
POLICY

1. Policy Brief

This policy (the "Policy") sets out: (a) the rules for the handling of data by Profound Medical Corp ("Profound") (b) acceptable use of computing devices by Profound personnel (including Personal Devices as defined below) for Profound business purposes; and (c) our approach to security-related incidents.

Profound is committed to respecting employee privacy in working life and governs itself according to applicable data protection legislations in countries it does business. Additionally, this policy is intended to inform "Users" of their responsibilities to protect Profound's technology and the information assets of the business. Profound's Information Technology function (IT) deploys cybersecurity and other software and systems to support the company's data protection objectives, and maintains the right to monitor, backup and if necessary, delete data from devices upon which the company's data is stored. As such, users should not conduct personal activities or store personal information on Profound Devices.

Profound protects its data while being accessed on a personal mobile device using Microsoft's MDM features. Enrolling a personal mobile device with Microsoft's Intune Company Portal is a requirement for accessing Profound's data on a personal mobile device. Controls are put in place to ensure that documents cannot be downloaded to personal mobile devices from Teams, OneDrive, SharePoint, and Outlook. Mobile Application Protection is enabled on all Microsoft applications which requires a separate 4-digit PIN entered by the user at the time of application launch. Profound reserves the right to monitor, and if necessary to protect Profound's data wipe all Profound's data from your personal device. By signing and agreeing to this document implies agreeing to the above conditions.

The purpose of this Policy is to:

- ensure the confidentiality, integrity, and availability of all Profound Information (as defined below) created, received, maintained or transmitted as appropriate.
- identify and protect against reasonably anticipated threats to the security or integrity of the information; and
- protect against reasonably anticipated, impermissible uses or disclosures; and ensure compliance with this Policy by Users (as defined below).
- provide transparency about Profound's electronic monitoring practices including technological, electronic, or digital means used to track, observe, or monitor actions.

2. Definitions

(i) "**Information**" means Profound Information and Non-Profound Information.

(ii) "**Internal Systems**" means Profound's e-mail and non-public information creation storage, transmission and management systems.

(iii) "**Non-Profound Information**" means any and all non-work related information created, sent, received, reproduced, processed, stored, transmitted and/or maintained by Users for personal use.

(iv) "**Personal Devices**" means non-Profound issued electronic devices, including mobile phones, tablets, laptops and desktop computers.

(v) "**Profound Information**" means any and all information, regardless of physical form or characteristic (including paper, electronic, audiovisual, microform, etc.), created, sent, received, reproduced, processed, stored, transmitted and/or maintained by Users and/or other persons acting on behalf of Profound in the ordinary course of their duties with Profound.

(vi) **"Users"** means employees, consultants and contractors of Profound authorized to use Profound Devices or Personal Devices.

(vii) **"TPM chip"** A Trusted Platform Module is a microchip that is often built into a computer to provide hardware-based security

(viii) **"MDM"** Mobile Device Management is a method of monitoring and exercising control over the mobile devices used by Profound Team members. MDM allows the enrollment, configuration, management and securing of both Profound and employee-owned mobile devices.

(ix) **"Electronic Monitoring"** means all forms of all employee monitoring that is done electronically.

3. Classification of and Access to Information and Systems

Profound acknowledges that different types of information will be subject to different levels of security controls based on the sensitivity of the information and the regulatory scheme applicable to such information. As such, Profound maintains a formal process for requesting, modifying and removing access to systems or networks used by its personnel to conduct Profound's business.

(a) Access to Systems.

Profound's access-provisioning process:

- addresses processes, procedures, and requirements relating to access to Profound Information;
- intends to ensure access permissions for each User are only to the extent required for such User to perform their assigned tasks;
- intends to ensure separation of duties to mitigate the risk of fraud, theft or misuse of Profound Information;
- ensures that User IDs are not shared between Users. So use or access of Profound Information can be tracked through usage reports; and
- de-commissions Users IDs that are no longer in use.

(b) Passwords.

All access to Profound Information and systems should be protected by passwords. In respect of password provisioning and maintenance, Profound:

- communicates to its Users password requirements designed to ensure the security of Profound Information and systems, including:
    - minimum requirements (length, mix of characters, biometrics, etc.); and
    - best practices with respect to storage of passwords; and
    - prevents or limits Users from further access after a number of unsuccessful attempts to gain access.

(c) Training.

All Profound personnel will receive training in order to facilitate compliance with this Policy as applicable to their particular role within Profound's business activities.

(d) Availability of Systems, Back Ups and Disaster Recovery

All Profound servers are backed up daily and data is archived indefinitely in the cloud.

(e) Encryption

All USB keys in the field used to transfer data will be encrypted using Windows Bit Locker technology.
All Profound provided laptops will be encrypted with Windows Bit Locker technology along with the laptop's TPM chip.

(f) Malicious Software

All machines connected to the Profound corporate network will have up-to-date Anti-Virus/Anti-Malware/Anti-Spyware software installed.

(g) Physical Security

Profound uses a risk-based approach to physical security that involves the identification, assessment, and management of security risks that may lead to the compromise of Profound's systems and Profound Information.

(h) Incident Management.

In the event any Profound Personnel becomes aware of any loss, destruction, misuse or misappropriation of Profound Information or unauthorized access to Internal Systems, the person who first becomes aware of such incident will contact the IT Department who will work in conjunction with HR as soon as reasonably possible and provide any relevant information about the incident as is known at the time. The IT Department will take reasonable steps to respond to the incident, including:

a) Considering at the outset the need to preserve evidence. Retain copies of logs, emails and other communications. For example, copies of malicious files may need to be preserved and quarantined instead of deleted.

b) Maintaining all documentation surrounding every security incident, including all working papers, notes, incident response forms, meeting minutes and other items relevant to the investigation in a secure location, under the control of legal counsel whenever possible.

c) Ensuring responsibility for documenting is clear and that only authorized persons review logs, interview witnesses, look for gaps, etc.

d) Considering at the outset whether a bad actor may have continuing access to our system. If so, consider whether to avoid taking steps that would alert them to the fact that we are aware of the breach.

e) Once an incident is resolved, debriefing and reflecting on the incident, response to the incident and lessons learned.

f) Creating a final incident report including recommendations for possible improvements to systems or processes or other measures that could reduce the risk of future security incidents.

4. Use of a Profound Device

(a) Care and Control

Users are responsible for any Profound Device while it is in the User's possession.

In vulnerable situations, e.g. public areas such as airport lounges, hotels and conference centers, Profound Devices must never be left unattended.

When using a Profound Device in a public place, Users must ensure that third parties cannot see the screen contents.

(b) Personal Use

Use of Profound computers or laptops should only be for personal use within reason.

Users are not permitted to use personal email addresses for business related purposes, including sending Profound Information to a personal email address.

(c) Use Restrictions

Users are not permitted to copy or export Profound Information to unauthorized devices, file-sharing sites or removable media (USB storage, other computers, Dropbox, Google Drive, etc.). The authorized file sharing transfer and storage services at Profound are **OneDrive for "Business**", encrypted USB sticks (whenever possible) and Profound's secure file transfer system.

Users may not use Profound Laptops/Computers or Internal Systems for the following:

- To download or exchange non-business files for personal use.
- To download or exchange games or entertainment software or to play games over the Internet.

Users may not use Profound Electronic Devices including Laptops/Computers Phones and Tablets or Internal Systems for the following:

- To download, exchange or view sexually explicit or offensive material.
- To further any form of harassment or offensive conduct, including but not limited to on the basis of a prohibited ground of discrimination;
- For personal profit or gain outside the User's work for Profound.
- To represent the User as someone else.
- To make defamatory or other comments that would reflect poorly on Profound.
- To hack into another system or Profound's Internal Systems.
- To participate in any illegal activity; or
- Any use that could damage Profound's business or reputation.

(d) Downloads and/or Streaming

Excessive streaming or downloading of any kind of media content using Profound Devices or Internal Systems is prohibited for non-business related purposes.

(e) Usage Reports

Mobility services usage reports may be used to verify that Profound Mobility Devices are being used appropriately and within Company guidelines.

(f) Access and Ownership of Profound Devices and Information

Profound Devices, and any Information contained thereon, are the property of Profound and as such are subject to Profound review, interception, collection, monitoring and access. Upon request by Profound, Users will provide Profound with full access to any Profound Device in their possession and all Information contained thereon. Users of Profound Devices are strictly prohibited from altering or deleting any Information contained on a Profound Device following a request by Profound to access the Profound Device.

(g) Loss of Eligibility

Profound Devices must be returned in the following circumstances:

- When a User's employment by Profound is terminated for any reason, including resignation.
- When a User takes a leave of absence, including legislated leaves
- (e.g., maternity leave), personal leaves in excess of 30 consecutive days, and long-term disability leaves;
- At Profound's discretion including if a User fails to comply with the Policy, or if Profound has reason to suspect any improper use of a Profound Device.

5. Use of Personal Devices

(a) Although not encouraged to do so, employees, contractors or consultants authorized to access Internal Systems may use personal electronic devices, including tablets, for Profound Business and if they agree to strictly adhere to this policy and enroll the specific device in the Microsoft's Intune Company Portal.

(b) Personal Use

Use of Personal Devices for personal reasons during business hours should be kept to a minimum and should not interfere with Profound's business. The nature and/or context of any personal use of a Personal Device must make clear to outsiders that the User is not representing Profound.

(c) Use Restrictions

Personal Devices and passwords or other credentials for Personal Devices must not be shared with third parties, including family members or friends, to prevent such third parties from gaining unauthorized access to Profound Information. All Profound information may only be stored on a personal device through the use of One **Drive for "Business."** Users are not permitted to copy or export Profound Information to unauthorized devices, file-sharing sites or removable media (USB storage, other computers, or file sharing applications such as Dropbox etc.).

(d) Access and Ownership of Information on Personal Mobile Devices

Any Profound Information which is created, sent, received, reproduced, processed, or transmitted on Personal Mobile Devices, is the property of Profound. The User should not have any

expectation of privacy when using Personal Devices to access Internal Systems or to create, access, transmit, or otherwise engage with Profound Information as personal devices are discouraged for business use.

Profound may; access, collect, or review any Information on a Personal Device for the purpose of identifying, locating, or collecting Profound Information, or for other purposes related to investigations, potential violations of Profound Policies, employment terms or laws.

6. Downloading Software and Documents

Users who require an application to be installed on a Profound Device must obtain advance authorization.

Downloading of software should only be done from reputable/vendor websites. i.e. Adobe products should only be downloaded from Adobe's website. Microsoft software should only be downloaded from Microsoft's web site.

Applications downloaded to Smartphones should only be done from one of the following:

Apple's App Store

Google Play

The Microsoft Store

7. Electronic Monitoring

Profound values trust, discretion and transparency, and believes all employees deserve to know when and how their work is being monitored whether in the workplace, at home, travelling or a hybrid work location model.

(a) Electronic Monitoring Practices

Profound's electronic monitoring resources, software and equipment are used for reasonable business and operations purposes including regulatory compliance, facility access and security, investigating compliance with internal policies and country specific legislation and regulations.

The company will adhere to any monitoring, privacy and legislation that applies to the collection, use, and disclosure of information obtained by electronic monitoring in which it does business.

All information collected through electronic monitoring is securely stored and protected.

(b) What Information is Collected and How It May Be Used

Profound currently electronically monitors whether directly or indirectly episodically or as needed the following assets, systems and or services**:**

Details	Information/ data collected	Purpose
1. Active Directory	The Active Directory is used to monitor devices connected to Profound's systems and the software productivity tool-event log which tracks the creation, modification and deletion of user accounts and computers, and when required; it also is used for restoring deleted objects and rolling back unwanted changes.	Used for Regulatory Compliance purposes (GDPR, HIPPA, and SOX); and to identify if any IT employee questionable activities.
2. Device Monitoring	Device monitoring includes capturing the following: -**File downloads** (SharePoint and OneDrive for Business) -**File activities** (Create, Copy, Move, Delete and Modify) of files located on Profound Medical's Files server, Profound Medical devices, and USB drives. -**Login and Logoffs** (including failed logins) to company systems (Network, VPN, Devices), online resources, applications and software. - **External IP address** that the employee is accessing Profound 's resources from. - Web browsing is NOT monitored, however accessing sites deemed restricted are be monitored.	Data collected may be used for auditing activities of any questionable internal behaviors in these areas.
3. Electronic Key Fob/Card	This electronic sensor creates a record each time an authorized employee scans their card when entering building or restricted areas such as the server room. The sensor retains data logs of physical access attempts, date and time of request to access	The purpose is to ensure both building and network security, as well as employee physical security, health and safety.
4. Communication Systems and Tools	All communications sent through Profound's technology tools are subject to auditing which includes Microsoft Office, HRIS, **email, and chat groups**. This includes personal email accounts when those accounts are accessed using a Profound Medical device.	Data collected is for the purpose of auditing activities for any questionable internal behaviors in these areas.
5. Network Security Tools	The following tools are utilized to ensure all digital assets are protected. The data gathered from these passive monitoring tools are to detect any risks. They are deployed on all device and workstations and enterprise wide for the network. protected, deter detect cybersecurity incidents. **-VPN** - OpenVPN **-Anti-Virus /malware** **-Firewall** **-IT security tools** (Cybersecurity, spam phishing etc.) -**Microsoft 365**	Network security tools are used to monitor the use of, and access to, Profound's systems and networks to detect any risks and cybersecurity incidents.
6. Video Camera System	The visible cameras and DVR system video captures, and records activities and movement in specific areas of office building and parking lot (all entrances/ exits, front lobby, Profound's server room, IT storage room).	Physical security – purpose is to protect the health and safety of our employees, outside and inside the office building; the system is also used for protecting Profound's assets

8. Damaged, Lost or Stolen Devices

Damage, loss or misappropriation of Profound Devices and Personal Devices covered by this Policy must be immediately reported, to ensure that appropriate security measures can be taken. Users must immediately report any incident or suspicion of unauthorized access or disclosure of Profound Information. BYOD Personal Devices must have remote location and information deletion (wiping) capabilities enabled at all times.

Such incidents must be reported as follows:

Kalvin Stubbs – Manager IT (Kstubbs@Profoundmedical.com) x411

Imad Nakaweh - IT Specialist (INakaweh@Profoundmedical.com)x405

Magdalena Gorkiewicz – Manager HR Operations (MGorkiewicz@profoundmedical.com)

9. Compliance

IT will work with the Manager HR Operations to ensure a country's National Legislations are respected.

IT will refer any requests from managers for access to recorded or stored information to the Manager HR Operations for review and approval prior to granting access.

Any User who fails to comply with this Policy may be subject to disciplinary action, up to and including termination of employment.

10. Revision History

Revision	Author & Approval	Revision Description	Effective date
1	M. Belza	Initial release.	
2	Author - IT **Approval** Aaron Davidson	Updated Release	Jan 2019
5	Updated K Stubbs **Approval** Rashed Dewan	• BYOD Program cancelled and policy updated to reflect this change • Contacts updated • Revision history chart added	Oct 2022
6.	Updated M Belza & K. Stubbs Approval Rashed Dewan	• Re-named Cybersecurity Policy to Cybersecurity and Electronic Monitoring Policy • Section 1 - bullet added to Policy Purpose - on Profound's Electronic Monitoring practices • Added a definition for Electronic Monitoring in Section 2 • Added "New" section (7) Electronic Monitoring	Feb. 9, 2023

Attachment:

Appendix A – Policy Acknowledgement and Sign-off Form

Appendix A

PROFOUND MEDICAL CORP.

CYBERSECURITY and ELECTRONIC MONITORING POLICY

Acknowledgement and Sign-off

I acknowledge receipt of the **Cybersecurity and Electronic Monitoring Policy.** I confirm that I have read and fully understand the contents of the policy and my responsibilities as an employee of the Company.

By my signature below I agree to comply with the policy as a condition of my employment and my continuing employment at Profound Medical Corp.

I understand that if I have questions, at any time, regarding this policy that I will consult with one of the following:

Kalvin Stubbs – Manager IT (Kstubbs@Profoundmedical.com)

Magdalena Gorkiewicz -Manager HR Operations (MGorkiewicz@profoundmedical.com)

Rashed Dewan - CFO (rdewan@profoundmedical.com)

Employee Signature:_____ Date_____

Print Name: _____