Contents

1. Purpose and Scope

1.1. The purpose of this policy is to describe the protocol of using the computing resources of Thorlabs Inc., 43 Sparta Avenue, NJ 07860, USA, and each of its direct and indirect subsidiaries and divisions[1] (collectively **"Thorlabs"**, **"we"** and **"our"**) in support of our business compliance requirements.

1.2. The scope of this policy is:

1.2.1. to help all worldwide Thorlabs employees (**"you"**) using tools and resources such as Computers, Software, Portable Media, Network/Internet access, Phone etc., to achieve your business objectives/goals;

1.2.2. to help you understand what Personal Information (as defined in section 2.8 below) of yours we collect and how we process that Personal Information; and

1 Including without limitation Thorlabs GmbH (Munich, Mittweida, Karlsruhe and Lübeck, Germany), Thorlabs Ltd. (Ely, UK); Thorlabs Elliptec GmbH (Dortmund, Germany), Thorlabs AB (Mölndal, Sweden), Thorlabs Japan, Inc. (Tokyo, Japan), Thorlabs SAS (Maison-Laffitte,, France), Thorlabs Vendas de Fotônicos LTDA (São Carlos, Brazil), Thorlabs Canada ULC (Montreal, Canada), Thorlabs Optical Electronic Technology (Shangai) Company, Ltd. and Thorlabs (Shanghai) Trading Company Limited (Shanghai, China), Thorlabs Quantum Electronics, Inc. (Jessup, Maryland), Maxion Technologies, Inc. (Jessup, Maryland), Thorlabs Lens Systems, Inc. (Rochester, New York), Thorlabs Imaging Research Group, LLC (Sterling, Virginia), Thorlabs Measurement Systems Inc., (Blairstown, NJ), Thorlabs Advanced Imaging Business Unit (Sterling, Virginia), Thorlabs Ultrafast Optoelectronics Business Unit (Ann Arbor, Michigan), Vytran (Morganville, NJ and Exeter, UK), Thorlabs Spectral Works (W. Columbia, SC), Thorlabs Crystalline Solutions (Santa Barbara, CA), and Thorlabs Laser Division (Boulder, CO)

1.2.3. to help you protect the security and privacy of Personal Information as well as corporate and other business confidential information that you may handle during your employment by Thorlabs.

You are required to accept and acknowledge this policy as a condition of your employment.

2. Definitions and Acronyms

2.1. **ISO** – Information Security Officer
2.2. **System** – Network Devices and Applications
2.3. **BUL** – Business Unit Leader
2.4. **GM** – General Manager
2.5. **DPO** – Data Protection Officer (Contact Information)
2.6. **Data Protection Laws –** means (a) all applicable US data protection laws; (b) European Union Directive 95/46/EC, the EU General Data Protection Regulation, as such regulation may be amended ("GDPR") and any legislation and/or regulation implementing or made pursuant to them including but not limited to: (i) the UK's Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2013; and (ii) the German Bundesdatenschutzgesetz (BDSG); (iii) the Swedish Dataskyddsförordningen; and (iv) the French Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée le 14 mai 2018 ; (b) US Department of Defense DFARS clauses including but not limited to: DFARS Subpart 204.73, DFARS 252.204-7012, and interim rule *Network Penetration Reporting and Contracting for Cloud Services* (DFARS Case 2013-D018) (collectively the "**DFARS**"); (c) for Japan: 個人情報保護法 (Personal Information Protection Law); (d) for China: Cyber-Security Law; and (e) any applicable associated or supplementary data protection laws, regulations, codes of practice or guidance, as updated, amended or replaced from time to time
2.7. **Data Subject** – means an individual who is the subject of personal data (i.e. the individual who is identified by the Personal Information)
2.8. **Personal Information** – any data relating to an identified or identifiable natural person

3. Security Responsibilities and Authorities

3.1. **Thorlabs Security Team** - Principal authority for all information security polices and system/application design. Oversee company use of the network resources to ensure business continuity. (Contact Information)
3.2. **DPO/ISO** - DPO will be appointed to the extent required by law. In the absence of a DPO, the ISO will fulfill the DPO's functions.
3.3. **GM/BUL Management -** Enforcement of Thorlabs polices as it applies to their business unit teams and processes.
3.4. **Incident Response Team -** Executive staff, IT, HR and other responders. (Contact Information).
3.5. **Employees -** Information Security is each and every employee's responsibility. Every employee shall be aware of the current policies, review these policies on an annual basis, and maintain compliance. Each employee is required to advise and supervise their vendors and consultants' compliance with our policy.

4. Policy

4.1. Regulatory and Security Compliance:

4.1.1. All systems must be maintained to comply with all applicable regulatory compliance requirements.
4.1.2. Security incident mitigation takes priority over any business service or function.
4.1.3. Where required, audits and remediation will be performed in accordance to local laws and regulations.

4.2. Privacy I: *How we handle your Personal Information*

4.2.1. We are the data controller for the purposes of all applicable Data Protection Laws.

4.2.2. **Information we collect:** We collect and process the following Personal Information about you:
(i) **Information that you provide to us:** This will include information that you provide to us when you join Thorlabs, for example, your name, address, phone number, date of birth, social security number or other information that you provide to us during the course of your employment;
(ii) **Information that you share:** This will include information that you share during your employment through any form or medium including, for example, the content of your emails or any posts on the intranet, internet, and any other form of electronic or social media platform;
(iii) **Information we collect:** This will include information that we collect from your use of Thorlabs Systems, including computer equipment, software, etc.

4.2.3. **How we use Personal Information:** We use your Personal Information for the following purposes:
(i) personnel administration, processing of payroll and benefits administration;
(ii) attendance data including absence days for contractual, performance, and payroll purposes
(iii) training and appraisal, including performance records and disciplinary records;
(iv) equal employment opportunity monitoring and compliance;
(v) E-mails with individual's names to customers, vendors, internal Thorlabs persons and outside stakeholders in the scope of the job assignment for facilitation of Thorlabs business
(vi) compliance with applicable procedures, laws and regulations;
(vii) identify the individual person in a recruitment process; and
(viii) any other reasonable purposes in connection with your employment.

4.2.4. **Data ownership:** Without limitation, but subject to compliance with the requirements of applicable law, all computers, data content, files, logs, email, etc. that are on or transverse the corporate network is the property of Thorlabs and can be audited/accessed at any time by authorized staff. This includes the content of any employees personal computing devices used to connect to the network and/or contain Thorlabs data content.

4.2.5. In the event there are personal email/files co-mingled with the corporate system, this content becomes the property of Thorlabs and is subject to review/audit as any other data content.

4.2.6. Email addresses and data, during active employment and after termination are considered Thorlabs intellectual property. After termination of the employee, the email addresses can only remain as an alias to the successor of the email address and not to be used as an active person. In the event of a new hire with the same user credentials, it may be reassigned with a new clean profile.

4.2.7. **Data Transfers:** As we are an international company, we may need to share your Personal Information with our offices located in another country from the one in which you are located. Any transfer of Personal Information outside of the country in which you are resident will be performed in accordance with the applicable Data Protections Laws and shall only be performed for the purposes specified in this Policy. **EU Employees:** Thorlabs complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union to the United States. The Thorlabs Online Privacy Statement may be accessed here. Any transfer of personal data outside of the European Economic Area to anywhere except the U.S. is for the purposes of satisfying contractual obligations and all such third parties receiving personal data are contractually bound to comply with Thorlabs privacy practices and to comply with the GDPR. Thorlabs recognizes potential liability in cases of onward transfer to third parties. Thorlabs complies with the Privacy Shield Principles for all onward transfers of personal data from the EU, including the onward transfer liability provisions. Thorlabs has certified to the Department of Commerce that is adheres to the Privacy Shield Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

4.2.8. **Data Retention:** We will retain and use your Personal Information for as long as you remain employed by us. In the event that your employment with Thorlabs ceases, your Personal Information will no longer be processed by us other than for legal or regulatory compliance reasons. We will retain your Personal Information for ten (10) years to ensure compliance with legal obligations and for business continuity and/or disaster recovery purposes. After this period we will destroy or delete the Personal Information to the extent that we are technically able to do so. An archival copy may be maintained in our archival system for compliance purposes consistent with our data retention policies, and processing activities on that data will only be performed for that purpose. The archival system shall only be accessible to a limited number of Thorlabs administrators in our worldwide organization.

4.2.9. **Data Minimization**: Thorlabs limits the type of Personal Information collected from employees to the minimum of information required to fulfill the purposes set forth in Section 4.2.3.

4.2.10. **Data Security**: Thorlabs will take reasonable precautions to protect Personal Information in its possession from loss, misuse, and unauthorized access, disclosure, alteration, and destruction, taking into account the risks involved in the processing and the nature of the Personal Information. Data containing highly confidential information (such as salary information or performance appraisals) are accessible only by designated managers who have received data security training. Personal Information contained in the Thorlabs Enterprise Resource Planning system is access protected by permissions assigned by the respective Human Resources Department. Thorlabs uses encryption when transferring sensitive Personal Information between Thorlabs entities and the Thorlabs IT security architecture prevents unauthorized access from users outside of Thorlabs. However Thorlabs does not guarantee that unauthorized third parties will never defeat measures taken to prevent improper use of Personal Information. Business continuity is secured through the Disaster Recovery Procedures and Back-Up Policy and procedures. Security assessments are performed regularly by Global IT periodically. The detection, analysis, prioritization and handling

of information security incidents, such as data breaches, will be managed in accordance with the Thorlabs Incident Response Plan.

4.2.10.1. Authorized personnel must have, and do have, controlled access to certain information stored on Thorlabs equipment. Thus, Thorlabs cannot guarantee the privacy of documents and messages stored by you in Thorlabs physical files, desks, physical storage areas, voice or electronic media so please do not share any Personal Information in these formats or on these devices that you are not willing for us to have access to. A review or search of these areas may occur without prior notice. The contents of communications or documents reviewed or retrieved by Thorlabs for legitimate business reasons may be used and disclosed without your permission but, to the extent they contain any Personal Information, shall only be disclosed in accordance with the terms of this policy.

4.2.11. **Required Disclosure:** Thorlabs may be required to disclose Personal Information in compliance with applicable procedures, regulations, and laws or in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

4.2.12. **Your rights to Personal Information:** You are entitled to receive a copy of the Personal Information that we hold about you. If you want us to supply you with a copy of the Personal Information which we hold about you, you should put a request in writing to the applicable contact. Your request should set out precisely what information it is you require (such as your performance reviews, your contract of employment, your health records etc.) and any dates that are relevant to the information you would like to see. You may be required to pay a fee for obtaining such information, in accordance with the level set by the applicable Data Protection Laws. We will endeavor to respond promptly to the request and in any event within 45 days (or other applicable time period required by Data Protection Laws) following our receipt of your request. If you would like, we can also provide you (or, where technically feasible, a specified third party) with a copy of any of your Personal Information that we hold.

4.2.13. **Your right to rectification:** If, once you've spoken with us, you find out that the Personal Information that we hold about you is incorrect or incomplete, please let us know and we will correct any mistakes.

4.2.14. **Your right to erasure:** If you want us to stop using or to delete your Personal Information, you can contact us and tell us why. In certain circumstances we may not be able to stop using your Personal Information but, if that is the case, we'll let you know why.

4.2.15. **Queries/Complaints:** If you wish to speak to us in relation to any of these rights, please contact the applicable **DPO/ISO**. The **DPO/ISO** is responsible for managing all requests for access to information, completing Thorlabs' annual registration, and overseeing communication about data privacy issues (both internally and externally). If you believe that we are not managing your complaint correctly, you may complain to your relevant data protection authority ("DPA") (a list of EU DPAs can be found here: https://edpb.europa.eu/about-edpb/board/members_en and, in the US, you can contact the FTC).

4.2.16. **Privacy Shield Complaints.** In compliance with the Privacy Shield Principles, Thorlabs commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Thorlabs at:

Email: privacy@thorlabs.com;

Telephone: 973-300-3000
Postal Mail: Attn: Information Security Officer
Thorlabs, Inc.
43 Sparta Avenue Newton, NJ 07860

4.2.16.1. Thorlabs has further committed to cooperate with the panel established by the EU DPAs with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship. A list of EU DPAs can be found here: https://edpb.europa.eu/about-edpb/board/members_en. The Federal Trade Commission has jurisdiction over Thorlabs' compliance with the Privacy Shield. If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

4.3. Privacy II: *How you should handle Personal Information*

4.3.1. Thorlabs appreciates the importance of privacy and we want to ensure that you understand how Personal Information should be treated in order to protect the privacy of Data Subjects, whether they are a customer, vendor or a colleague.

4.3.2. **Key requirements:** You must comply with the principles set out below with regard to Personal Information relating to employees, other personnel, vendors, clients and other people about whom we hold Personal Information.

Personal Information must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

4.3.3. **Data Subject Access Requests:** If you receive a subject access request from someone outside of Thorlabs, such as a client, for a copy of their Personal Information you should first pass the

request to the applicable DPO/ISO who will instruct you how to respond or will respond to the request on your behalf.

4.3.4. If you believe that another employee may have infringed this Policy, please discuss this with your line manager.

4.3.5. If you have any doubts about whether you are processing Personal Information fairly and lawfully, you should contact the DPO/ISO before doing anything with that Personal Information.

4.3.6. **Data Breach:** If you suspect that there has been any breach of Thorlabs IT security, you must immediately notify the Incident Response Team. Please include all relevant information in your notification, for example, the suspected cause of the breach and the categories and types of any Personal Information that may have been lost, altered, deleted, disclosed or accessed.

4.4. Acceptable Use and Ethics

4.4.1. Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, provincial or international law while utilizing corporately-owned resources.
4.4.2. System users who receive a username and password must keep that information confidential and not allow use of their account by others.
4.4.3. System users who leave their workstations should enable the lock screen or log off to prevent unauthorized access.
4.4.4. Employees shall not post or represent Thorlabs in any public forum or media, unless it is their role and have been authorized to do so.
4.4.5. System users must not tamper with or disable anti-virus or other required company software installed on their workstations.
4.4.6. System users are prohibited to install any software on their workstations without prior approval from IT management.
4.4.7. Email users must be very careful when opening email attachments, and should be cautious with unsolicited emails containing attachments, especially when coming from unverified sources.
4.4.8. System users must not reveal any information about corporate clients, employees, business practices, technology, schedules, or any other information not already publicly available to any outside resource or person without expressed permission from their supervisor.
4.4.9. System users must not use their corporate email accounts, or other communication tools, for purposes other than the conduct of corporate business. Forbidden actions include any and all forms of harassment, phishing, solicitation, spamming, forwarding chain letters and pyramid schemes, conducting personal business, and general personal correspondence.

This document will be reviewed by the policy owner periodically for compliance with policies, standards and any other requirements.

4.5. Non-Acceptable Use

Includes but not limited to the following:
4.5.1. Excessive/frivolous use of resources for non-business related purposes including: internet browsing, Social Media, IRC, Instant Messaging, stock tickers, personal email, video/audio streaming, and news-boards.
4.5.2. Communication and/or upload/downloading of illegal, inappropriate or distasteful content.

4.5.3. Spamming, which includes but is not limited to: sending unsolicited mass/bulk emails that could provoke complaints from recipients.

4.5.4. Accessing, altering or destroying information or devices of any third party or attempt or experimentation to do so.

4.5.5. Use of any service or technology that disguises/proxies employee activity.

4.5.6. Use of internet service or technology to connect, interface, or interact directly with any Thorlabs system.

4.5.7. Any attempt to access, read/write/review, decompile/decode, capture, redirect, spoof, impersonate, copy, circumvent security and infrastructure solutions, do intentional harm to any data systems or services not directly related to their role is considered trespassing, and a serious breach of security. Unauthorized access or tampering of such material may result in severe disciplinary action as well as substantial civil and criminal penalties; and be held accountable under national, state, and federal Economic Espionage laws.

4.5.8. System users may not perform vulnerability scans, monitor network traffic, or perform any action that is designed to elevate privileges or gain access to information that was not expressly intended for them.

4.6. Use of Corporate Network Resources

4.6.1. Only authorized computers and configurations are permitted on the corporate network. All issued computers are required to be domain machines and centrally configured and managed by the backend systems. Devices used must be models and operating systems supported/approved by the organization.

4.6.2. Alternate equipment can be used for special research and development needs based on approval from the Security Team before use in the Thorlabs environments. Support is limited and best practices and current guidelines should be supported.

4.6.3. Any network/data enabled device planned for use at Thorlabs must be reported to the Security Team for review of security concerns, measures, and compatibility/support evaluation. They must be approved prior to purchase and deployment.

4.6.4. Employee owned, computing devices are not permitted, nor will be supported, on the company network unless authorized by a security team member.

4.6.5. Employee issued computer/devices shall be used by Thorlabs employees only, as assigned to them. Non Thorlabs employed staff shall not use the device (specifically all friends, family members, and business affiliates). Accessibility of the device is the responsibility of the employee.

4.6.6. Use of memory sticks, USB drives, backups to disk or other media is permissible for business use if authorized. Content shall not be removed from the premises without authorization from the owner/principle of the content or in conjunction with your business role and responsibility.

4.6.7. Use of any hot spot wireless device is prohibited unless issued by IT. (ie: 3G/4G, edge cards, android/iPhone devices in hot spot modes, portable internet devices etc.). These devices do interfere with the existing enterprise environments and can lead to network breaches.

4.6.8. Any computer/device used for remote access of company assets, not including public portions, must comply with corporate configuration guidelines.

4.6.9. Remote access software must use encrypted communications, be configured to use unique usernames and passwords for each user, and have any other security featured enabled.

4.6.10. No employee or manager may have access to another employee's email without explicit permissions from executive management and the DPO/ISO. This does not apply to department/workgroup shared mailboxes.

4.6.11. Any plans for development or production hardware or software applications systems must be approved by the applicable IS group, security group, and deployed according the standards and requirements.

4.7. Password Policy

4.7.1. Encrypted passwords should be enabled on any devices where it is not on by default.
4.7.2. Each corporate user should have a unique username and password that is not shared with any other user.
4.7.3. Corporate account passwords shall be set to expire and automatically prompted to be changed at least every 90 days.
4.7.4. A corporate accounts password should be strong and unique from previously used passwords.
4.7.5. Accounts shall be locked after 3 password failures and will auto reset after 30 minutes.
4.7.6. Request password change if there is any suspicion that your account has been compromised or the password is exposed to anyone.

4.8. Business Intellectual property

4.8.1. Any data shall be stored or transferred through Thorlabs provided services, where the content is protected and secured. This applies to, but not limited to: use of third party web applications, file exchange, web site hosting, email services, application programs, etc. Contact the Security Team for approved methods of large file exchange.
4.8.2. All high level classified documentation/data shall be stored on the provided network systems specifically items subject to review, audit, permanent record etc.
4.8.3. All end user data requiring backup or protection, shall be stored on the provided network file repositories. Local computer workstations are not in scope of our data backup policies.
4.8.4. No data, electronic or printed, or copies thereof, shall be removed or stored outside the organization unless at an approved resource.
4.8.5. Unless expressly authorized to do so, staff are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to Thorlabs. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal Economic Espionage laws.

4.9. Disciplinary Action

4.9.1. Infractions of any guidelines may result in disciplinary action up to and including termination of employment. If necessary, Thorlabs will advise appropriate legal officials of any illegal violations.
4.9.2. Any employee who discovers a violation of this policy shall notify the Security Team and/or Human Resources Department. Any employee who has a question concerning the interpretation of these policies should contact the Security Team, HR, or Executive Management.

5. Revision History

Revision	Effective Date	Description of Change	Revision Originator
		Comprehensive IT Security Policy V1.0	T. Klose, A. Lepore T. Lytken

1.0	5/24/18	Separated into external and internal document to comply with GDPR -> V1.0 of this document	D. Jennrich, V. Levy, R. Regimbal
2.0	7/1/19	Updated §4.2.7 and §4.2.11 to further align with EU-U.S. Privacy Shield principles	V. Levy, R. Regimbal
2.1	6/10/20	Updated covered entities and divisions to add TMS, Inc., TSW, TCS, & Thorlabs Laser Division - Boulder	V.Levy, R.Regimbal
3.0	6/16/20	Added new §4.2.16 and §4.2.16.1 in accordance with EU-U.S. Privacy Shield principles	V.Levy, R.Regimbal
4.0	6/1/21	Updated §§4.2.7 and 4.2.16.1 to further align with EU-U.S. Privacy Shield principles	C. Russo, R. Regimbal
5.0	3/25/22	Updated §§3 and 4 to correct a misprint and reference new technologies	C. Russo, R. Regimbal, T. Klose
6.0	1/17/23	Updated to amend business address and subsidiaries	C. Russo, R. Regimbal