## 1. Purpose and Scope

1.1. The purpose of this policy is to describe the protocol of using the computing resources of Thorlabs Inc., of 43 Sparta Avenue, New Jersey 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. explain the Thorlabs data security policy to our Business Partners
1.2.2. to help you understand what Personal Information (as defined in section 2.6 below) of yours we collect and how we process that Personal Information.

## 2. Definitions and Acronyms

2.1. **Business Partners** – Thorlabs customers, service providers, contractors, agents, and suppliers
2.2. **ISO** – Information Security Officer (Contact Information)
2.3. **DPO** – Data Protection Officer. (Contact Information)
2.4. **Data Protection Laws –** means (a) all applicable United States 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 United Kingdom Data Protection Act 2018 and the United Kingdom Data Protection Regulation, as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018; (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), 行政手続における特定の個人を識別するための番号の利用等に関する法律 (Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures); (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
2.5. **Data Subject** - means an individual who is the subject of personal data (i.e. the individual who is identified by the Personal Information)
2.6. **Personal Information** – any data relating to an identified or identifiable natural person

*1 Including without limitation Thorlabs GmbH (Munich, Mittweida, Karlsruhe and Lübeck, Germany), Thorlabs Ltd. (Ely, United Kingdom); 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), Thorlabs Lens Systems, Inc. (Rochester, New York), Thorlabs Imaging Research Group, LLC (Sterling, Virginia), Thorlabs Measurement Systems Inc., (Blairstown, New Jersey), Thorlabs Advanced Imaging Business Unit (Sterling, Virginia), Thorlabs Ultrafast Optoelectronics Business Unit (Ann Arbor, Michigan), and Vytran (Morganville, New Jersey and Exeter, United Kingdom), Thorlabs Spectral Works (W. Columbia, South Carolina), Thorlabs Crystalline Solutions (Santa Barbara, California), and Thorlabs Laser Division (Boulder, Colorado)*

## 3. Security Responsibilities and Authorities

3.1. **Thorlabs Security Team** - Principal authority for all information security polices and system/application design. Oversees 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. **Incident Response Team –** Thorlabs Executive staff, IT, HR and other responders. (Contact Information)

## 4. Policy

### 4.1. Regulatory and Security Compliance:

4.1.1. All systems are being 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 with local laws and regulations.

### 4.2. Privacy – How we handle Personal Information of our Business Partners

4.2.1. We are the data controller for the purposes of all applicable Data Protection Laws. (Contact Information)

4.2.2. **Personal Information we collect and process from our Business Partners:**
(i) **Information that you provide to us:** This includes but is not limited to information that you provide to us when you e.g. ask for technical support, submit a request for quote, place an order, submit delivery information, place a request for RMA, open an e-commerce account etc.: Your company name, your name, e-mail address, phone number, delivery and invoicing address;
(ii) **Information that you share:** This will include information that you share with Thorlabs for example, the content of your emails or any posts on our website or 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, e.g. your order statistic with Thorlabs, the number of contacts associated to your company etc.

4.2.3. **How we use Personal Information:** We use your Personal Information for the following purposes but not limited to:
(i) On request, to inform and update about products and services;
(ii) Notify Business Partner referrals of Thorlabs services, information, or products when a Business Partner requests that Thorlabs send such information to referrals;
(iii) Realizing contractual preparation and execution of sales and purchase of products and services (quotes, order confirmations, delivery documents, invoices etc.);
(iv) Complete a transaction, or provide services or customer support;
(v) Allow the purchasing of products, accessing of services or otherwise engage in activities on Thorlabs websites

(vi) Ensuring compliance with legal obligations and Business Partner's quality system (quality agreements with names of responsible persons, confirmations of compliance, non-disclosure agreements, etc.);
(vii) Communicate with the Business Partner;
(viii) Improve services, information, and products;
(ix) Notify of any changes with a Thorlabs website which may affect a user;
(x) Enforce the terms of use on a Thorlabs website;
(xi) Resolve disputes

4.2.4. **Legal Basis for Processing and Data Transfers:** The legal basis for the processing of our Business Partners' Personal Information is GDPR Article 6 (1)(b). On the basis of Article 6(1)(f) (legitimate interest), we process data in order to make our website available, to improve our products and/or to inform our Business Partners about similar products and services. Processing on the basis of a legitimate interest allows you as the Data Subject, in accordance with GDPR Article 21(1), to object to processing of Personal Information at any time on grounds related to your individual circumstances. Thorlabs processes Personal Information related to our entire supply chain on servers located in the United States. For logistics reasons we may need to share your Personal Information with logistic companies and/or 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, specifically GDPR Article 44 (and shall only be performed for the purposes specified in this Policy).
**Individuals Located in the EU or UK:** Thorlabs and its subsidiaries in the United States, Thorlabs Imaging Research Group, LLC, Thorlabs Quantum Electronics, Inc., Thorlabs Measurement Systems Inc., and Thorlabs Lens Systems, Inc., adhere to the EU-U.S. Data Privacy Framework Principles and all processing in the United States will be in accordance with the EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework. The Thorlabs Online Privacy Statement may be accessed here. Any transfer of personal data outside of the European Economic Area or United Kingdom, as applicable, to anywhere except the United States is for the purposes of satisfying contractual obligations and all such parties receiving personal data are contractually bound to comply with Thorlabs privacy practices and to comply with the GDPR.

4.2.5. **Data Retention:** We will retain documents with your Personal Information for the period we are legally required to maintain data. 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.

4.2.6. **Data minimization**: Thorlabs limits the type of Personal Information collected from Business Partners to the minimum of information required to fulfill the purposes set forth in Section 4.2.3.

4.2.7. **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. Your Personal Information in our Enterprise Resource Planning system is restricted to Thorlabs administrators and employees on a need-to-know basis. Any information marked as confidential is stored in access protected storage places. Thorlabs uses encryption when collecting or transferring

sensitive Personal Information 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 the Back-Up Policy and procedures. Security assessments are performed regularly by Corporate IT periodically.

4.2.8. **Security on our e-commerce site**: Please refer to our Online Privacy Statement.

4.2.9. **Password Policy:** User passwords are keys to accounts. Each user should have a unique username and password that is not shared with any other user. Use unique numbers, letters, and special characters for passwords and do not disclose passwords to other people in order to prevent loss of account control. Request password change if there is any suspicion that your account has been compromised or the password is exposed to anyone. Encrypted passwords are enabled on any devices handling Personal Data of our Business Partners.

4.2.10. **Your rights to Personal Information:** You may ask for further information about the processing of your Personal Information at any time. Please put a request in writing to the applicable contact. Your request should set out precisely what information it is you require 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 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.

4.2.11. **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.

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

4.2.13. **Your rights to restriction of processing:**

In accordance with GDPR Article 18 as the Data Subject, you have the right to demand that we restrict the processing of your Personal Information if one of the following conditions applies:

• You contest the accuracy of the Personal Information. Processing may be restricted for a period of time to allow us to verify the accuracy of the Personal Information.

• The processing is unlawful, you refuse to delete the Personal Information and instead request the processing of Personal Information be restricted.

• We no longer need the Personal Information for processing purposes, but you require us to assert, exercise or defend your rights in the Personal Information.

• You have objected to the processing in accordance with GDPR Article 21(1) and it is not yet certain whether our interests in processing the Personal Information is paramount.

4.2.14. **Your right to data portability:**

As the Data Subject, you have the right to receive the Personal Information that you provided to Thorlabs in a structured, common and machine-readable format. You also have the right to transfer this data to another Controller without hindrance by us, provided the processing is based on (i)

consent provided pursuant to GDPR Article 6(1)(a) or Article(9)(2)(a) or (ii) a contract in accordance with GDPR Article 6(1)(b) and processing is performed by means of automated procedures (unless the processing is necessary for the performance of a task in the public interest or in the exercise of public authority delegated to the Controller). Furthermore, in exercising your right to data portability, in accordance with GDPR Article 20(1), you have the right to obtain the Personal Information, if any, transmitted directly from us to another Controller, to the extent this is technically feasible and does not affect the rights and freedoms of other persons.

4.2.15. **Effects of not providing data:**
If you choose not to provide us with data necessary for the performance of a contractual relationship, we may not be able to perform certain critical functions including but not limited to order transactions, deliveries or payment processes. For these reasons, we may not enter into a contractual relationship with you or we may need to terminate any ongoing contractual relationships with you.

4.2.16. **Queries/Complaints:** If you wish to speak to us in relation to any of these rights, please contact the applicable DPO/ISO listed here. If we cannot resolve your complaint, EU individuals may complain to their relevant data protection authority ("DPA") (a list of EU DPAs can be found here: https://edpb.europa.eu/about-edpb/board/members_en), UK individuals may complain to the UK Information Commissioner's Office (ICO) (https://ico.org.uk/), Gibraltar individuals may complain to the Gibraltar Regulatory Authority (GRA) (https://www.gra.gi/), and U.S. individuals can contact the U.S. Federal Trade Commission

4.2.17. **Data Breach Incident Response:** 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. If we suspect that there has been any breach of Thorlabs IT security, we immediately apply our Incident Response Plan and will inform the Supervising Authority as required.