KYC POLICY

Identity verification and compliance requirements

KYC POLICY

INTRODUCTION

This KYC Policy is adopted by the legal entity hProof, incorporated under legislation, with the registered number 16316410 and having registered address at Harju maakond, Tallinn, Kristiine linnaosa, Mustamäe tee 6b, 10616, Estonia , which operates in providing outsourcing services, related to finding and providing cyber security specialists for the Clients all over the world.

Both international and local regulations require hProof to establish effective internal procedures and mechanisms to prevent possible violation of current international sanction regime, including violation of sanctions imposed by local governments, but having exterritorial force, mitigating the risks of possible facilitating in terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery, other negative consequences that might occur while providing the Services.

This Know Your Customer Policy (hereinafter - the “KYC Policy”) is designated to prevent and mitigate possible risks of hProof (hereinafter - the“ Company”) concerning the scope of Services provided by the Company.

This KYC policy sets the standards of conducting all necessary due diligence procedures to ensure that the Services provided by the Company were accurate and transparent in regard to conducting such procedures.

This KYC policy is developed as part of internal policies of the Company specifically for the use of designated persons of the Company, which are responsible for conducting KYC policy. It shall be used as a guideline/instruction while performing the KYC procedure.

KYC Policy covers the following matters:

1. TERMS AND DEFINITIONS

Company – hProof, an Estonian company, with the registered number 16316410 and having registered address at Harju maakond, Tallinn, Kristiine linnaosa, Mustamäe tee 6b, 10616, Estonia, eligible to provide the Services to the Clients according to the definitions set forth in these Section.

Scope of Services (may be also referred as - “Services”) – the main business activity of the Company. Such Services include, but are not limited to, Services of finding Specialists in the sphere of cyber security, information technology, penetration testing, site reliability, other related activity. The Company also conducts all necessary research on such Specialists before the further interaction with the Client.

Client – a legal entity or a private individual, entering into an agreement with the Company, within the Scope of Services stipulated in the definition “Scope of Services”.

KYC policy – internal set of rules, developed by the Company, in order to prevent and mitigate negative consequences, which might occur, while providing the Services. The Policy specifically designated to indicate diligent Cyber security specialists from malicious Cyber security specialists, often called “black-hat hackers”.

Cyber security specialists (hereinafter – “Specialists”) – general term used in the present KYC policy, corresponding to all Specialists, having professional skills in cyber security, information technology, network security industry and are subject to these KYC policy rules.

Enhanced Due Diligence - additional information, collected for the purpose of conducting intellectual analysis, in order to have a deeper understanding of a person's past and present activity to mitigate associated risks. For the Purpose of the present KYC policy EDD used on the Specialists, to differentiate the diligent Specialists from “black-hat hackers”, and to prevent negative consequences connected with that.

Sanctions regime – international and local legislation, connected with imposing restrictions, limitations, prohibitions, on Companies/Entities, suspected in the activity(-ies), subject to the current Sanctions regime.

“Black-hat hacker” – cyber security specialist, who violates computer security for personal gain or malice. For the purpose of the present KYC, the Black-hat hackers are also considered to be persons who had been working or connected with the persons or organization responsible for committing cyber security crimes, and are subject to the sanctions imposed.

Responsible persons of the Company – specially appointed persons of the Company to form the united system of verification of Cybersecurity Specialists, managing and overseeing necessary KYC/EDD checks and investigations conducted by the Company or its authorized KYC Subcontractor. By default, the main responsible person for the KYC procedure is the CEO of the Company..

By default, the main responsible person for the KYC procedure is the CEO of the Company.

Compliance Executive – the designated person of the Company in charge of making decisions, regarding the KYC/EDD check. The Compliance Executive may be appointed by the CEO of the Company and shall respond and report only to the CEO of the

Company. In the absence of the Compliance executive the decision making shall be up to the CEO of the Company which shall at all time act as a Compliance executive, without regard to the absence or presence of the Compliance Executive in the Company as a “position”

KYC Subcontractor (or Subcontractor) – a specialized third-party service provider engaged by the Company to conduct due diligence, identity verification, and screening procedures on behalf of and under the express instructions and control of the Company, in accordance with the standards set forth in this KYC Policy.

2. VERIFICATION PROCEDURES

One of the international standards for preventing illegal activity and mitigating possible risks while providing the Services is due diligence process (“EDD”). According to “EDD”, hProof sets its own verification and due diligence procedures within the standards of “Know Your Customer” frameworks to ensure that the Company has taken all reasonable steps, while conducting such “EDD” to prevent negative consequences for the Clients and for the Company itself.

The responsible person(s), either directly or by issuing instructions to the authorized KYC Subcontractor, shall follow the procedure laid down below when conducting EDD.

Identity verification

The Company’s identity verification procedure requires the Cyber security specialist (hereinafter - “Specialist”) to provide the Company with reliable, valid, up-to-date and accurate source of documents, data or information, which includes, but may not be limited to:

- National ID or another identity verification document,
- International passport,
- Bank statement for the past year,
- Tax declaration, if applicable, for the past 3-5 years,
- CV, work experience for the past 10 years.

The Compliance executive / Responsible person(s) **shall at all times request a National ID or another identity verification document of the Specialist along with its selfie with such ID document, for the purposes of Sanction lists screening subject to Section 4 of this KYC policy.**

Other documents, which are specified in the present Section shall be asked from the Specialist, if the Client of the Company, authoritative body, or other concerned party asks for it specifically. The package of documents that shall be provided to such a party is subject to negotiations between the Company and such a party and determined on a case-to-case basis.

The Compliance executive / Responsible person(s) shall ask for such information and receive it before giving to the Specialist any sort of access to the information, resources, credentials, etc..

While conducting Identity verification the Compliance executive/responsible person(s) shall take reasonable steps to confirm the authenticity of documents and information provided by the Specialist.

All legal methods for double-checking identification information of the Specialists may be used and exhausted by the Compliance executive / responsible person(s), along with its sole right to investigate certain Specialists, by asking to provide more additional information or data, in case such Specialists have been determined to be **risky or suspicious.**

The Specialist shall be recognized risky or suspicious, if he/she:

- Presents inconsistent/wrong/inaccurate data, which is in conflict with the other pieces of information, previously provided to the Company.
- Is subject to the Sanction lists, specified in Section 4 of this KYC Policy.
- Provides the information that indicates or may possibly indicate the reasons for denying cooperation, which are specified in Section 4 of this KYC Policy.

The Compliance executive / responsible person(s) shall verify the Specialist's identity on an on-going basis, especially when their identification information has been changed, or with regard to their past activity, when e.g.:

- the work history of the Specialist was suspicious (e.g. the companies the Specialist worked with may be subject to the sanction lists, or sanction regime violation, specified in Section 4);
- the inconsistency of the several pieces of data provided by the Specialists is discovered;
- the Sanction lists were updated.

For the above purposes the Compliance executive / responsible person(s) shall, where it is deemed necessary, request up-to-date documents from the Specialists, even though they have passed identity verification in the past and have successfully passed identity verification procedures. The renewal of the documents by the Compliance executive/responsible person(s) shall be conducted at least 6 months after first verification, except cases provided in this Section.

The Specialist's identification information shall be collected, stored, shared and protected strictly in accordance with the Company's Privacy Policy procedures and related regulations, as well as in accordance with the necessary measures specified in Section 7.

Outsourcing and Subcontracting of KYC Procedures

The Company reserves the right to outsource the gathering, processing, and preliminary analysis of identity documents and screening data to a designated KYC Subcontractor.

When a Subcontractor is engaged, the following rules apply:

- Company's Instructions: The Subcontractor shall perform all verification and screening checks strictly under the guidance, parameters, and instructions provided by the Company.
- Final Decision-Making: For the avoidance of doubt, the Subcontractor acts solely as an investigative and data-processing agent. The final decision regarding the risk level, approval, or denial of cooperation with any Specialist remains exclusively with the Compliance Executive and the CEO of the Company.
- Quality Control: The Responsible persons of the Company shall regularly monitor and audit the performance of the Subcontractor to ensure that the verification quality meets the standards of this Policy and applicable legislation.

3. APPLICABLE LEGISLATION

Whilst conducting due diligence and verification procedures in the areas of finding and recruiting Cyber security specialists, the Company and the Compliance executive / responsible person(s) shall rely on the legislation applicable to ensure that KYC and EDD process has been conducted in accordance with such legislation in order to prevent and mitigate the negative consequences that might occur for the Company and its Clients.

The acts applicable also entitles the Compliance executive / responsible person(s) to conduct research and investigation not only in terms of the identification of the Specialist but his/her former and present connections with the companies or persons that are subject to legislative restrictions imposed in the below mentioned acts.

That means that the Compliance executive / responsible person(s) not only has the legal right but legal obligation to check such information, concerning the legal entities or persons the Cyber security specialist was previously or is currently engaged with.

The legislation applicable to KYC procedures includes the following acts:

- Executive order 13694 of the President of the United States of America, dated April 1, 2015;
- Executive order 13757 of the President of the United States of America, dated December 28, 2016;
- Council Decision (CFSP) 2019/797 of the European Union;
- Council Regulation (EU) 2019/796 of the European Union;
- Council Implementing Regulation (EU) 2020/1744 of the European Union dated November 20, 2020;
- Financial sanction Notice of the Office of Financial sanction implementation of HM Treasury dated November 24, 2020.

While using such legislative acts as legal framework the Compliance executive / responsible person(s) shall use other additional acts, connected with implementing such acts as well as check against sanction lists specified in Section 4.

The list of such additional acts is following:

- Sanctions Brochures (overview of OFAC's regulations with regard to Cyber-related Sanctions) - https://home.treasury.gov/system/files/126/cyber.pdf
- Advisory on Potential Sanctions Risks for Facilitating Ransom ware Payments https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
- A Framework for OFAC Compliance Commitments - https://www.american-club.com/files/files/cir_33_19_p2.pdf
- Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States — https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

In the interactions with the Clients from the European Union, the Compliance executive / responsible person(s) shall apply the Council decisions and regulations of the European Union, mentioned above as prevailing before the sanctions imposed, e.g. by the US or other government. It means that the Specialist for the European Client shall comply with the EU legislation regarding sanction regime, devoted to cyber security crimes.

If the person is connected to the Companies or individuals, which are subject to OFAC sanctions list, but not European, this shall be considered as one of the risk factors for the Company and the Compliance executive / responsible person(s) shall address such issue to the CEO directly while presenting information on the Specialist.

Should the Specialist fail to comply with the legislation mentioned above, or in any other possible manner was or is connected with the persons or entities/group of entities, which are subject to limitations/restrictions, or any other sort of prohibitions, imposed on them by the above mentioned legislation, **the Company cannot continue to cooperate with such Specialists and shall deny him in such cooperation, and the Compliance executive / responsible person(s) shall expressly notify the CEO thereof. The latter shall take all the**

necessary measures to terminate the cooperation with such Specialists.

4. SANCTIONS LISTS SCREENING

The Compliance executive/responsible person(s) screens the Specialists against the recognized Sanctions lists.

The Sanction lists may not be usually connected with entities or Specially Designated Nationals (SDN persons), which were engaged in or connected to Cybercrimes. However, the Compliance executive/responsible person(s), while conducting due diligence process verifies and investigates the Specialist **against all recognized Sanction lists**. The Compliance executive/responsible person(s) conducts such investigation with the purpose of preventing negative legal consequences for both the Company and its Clients.

The recognized sanction lists related to cyber security crimes, which the Compliance shall use for KYC procedure, are the following:

- Annex to Executive order 13694 of the President of the United States of America https://home.treasury.gov/system/files/126/E.O.%2013694%2C%20as%20amended%2C.pdf
- Annex I to Regulation (EU) 2019/796 - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125&from=EN
- SDN List by OFAC (USA) - https://www.treasury.gov/ofac/downloads/prgrmlst.txt
- List of persons/organizations, which are subject to the “most wanted” Bureau of Investigation of the US - https://www.fbi.gov/wanted/cyber
- List of persons/organization wanted by Interpol -
- https://www.interpol.int/How-we-work/Notices/View-Red-Noticesby Federal
- Consolidated list of Financial Sanctions targets in the UK https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/937950/Cyber-Attacks.pdf

The lists have to be periodically reviewed due to their amendments that may arise. The periodic overview of sanction lists and current local and international sanction regime shall be conducted at least every 60 (sixty) calendar days.

The CEO of the Company shall appoint the responsible person(s) for such periodic review. That person may be the Compliance executive, with necessary legal and professional background to review the KYC procedure, monitor the sanction regime, both national and international specifically, in regard to the cyber security crimes, and making decisions in regard to the approval or denying possible Specialists for the Company.

The Compliance shall deny in further cooperation with the Specialist in the following cases:

- The Specialist worked for the entities/companies subject to the Sanctions lists, specified in the present Section.
- The Specialist received payments from the companies/individuals subject to the Sanction lists, specified in the present Section.
- The Specialist worked for the companies/entities, which violated the sanction regime, providing goods or services to the companies/entities subject to the Sanction lists.
- The Specialist received payments from the companies/entities and individuals, which violated the sanction regime, both local and international.
- Other reasons connected to the violation of the current international and local sanction regime, but not specified in the present KYC.

In order to perform the screening process, the Company uses special software tools and/or relies on the specialized verification systems of the engaged KYC Subcontractor, designated to check the information about the companies/persons subject to the Sanction lists. The responsible person(s) for choosing such software tools or evaluating the Subcontractor's systems shall be appointed by the CEO of the Company.

5. RISK-BASED APPROACH

The final decision on cooperation with the Specialist shall be built on a risk-based approach. That means that after getting all the required information from the Specialist, according to this KYC policy, the Company conducts an intellectual analysis of such data to ensure that it is accurate and does not carry threat/risk both to the Company and its Clients.

For the purpose of defining the Risk-based approach in the present KYC it is understood that the specialists of the Compliance executive or the persons responsible for conducting KYC shall consider **risk above all other factors.**

In case there are risk factors for the Company, which are not explicit at the moment, but may have negative legal or any other consequences for the Company, in the future, the responsible person(s) shall inform the Compliance Executive and the CEO about such risk factors for them to make a final decision.

6. LIABILITY

Responsible person(s) shall be liable for the wrong/incorrect actions, which were made due to errors, omissions of the facts, not diligent investigation, unprofessionalism, conspiracy, other reasons, that may occur and which resulted in negative consequences for the Company. The liability of the person shall be connected proportionally to the damages the Company had suffered. The decision as to the penalty for such a person shall be made by the CEO, and

and calculated according to the damages the Company had suffered. This liability extends to the failure of the Responsible person(s) to properly instruct, monitor, or review the performance of the engaged KYC Subcontractor.

7. CONFIDENTIALITY CLAUSE

The Compliance executive / responsible person(s) are responsible for the confidentiality of the data, information, provided to them by the Specialists.

The Compliance shall take all necessary precautionary measures in regard to the security of the data provided, as well as the process of its analysis, retention. The Compliance cannot forward or share any information regarding the verification of Specialists, specified in Section 2, its other personal data, to any third party, except for the authorized KYC Subcontractor processing data under the Company's instructions for verification purposes, or unless they are obliged to do so, by authorities or by law. Any data transfer to the Subcontractor must be strictly regulated by a Data Processing Agreement (DPA) and confidentiality terms. The decision to share or forward such information to other parties shall be made by the Compliance Executive with the CEO's approval.

The Compliance Executive or the responsible person(s) shall be in charge, as for the organizing the security, storage and confidentiality of the data/information, provided by the Specialists.

8. APPLICABLE LAW

The Estonian legislation shall govern all disputes and/or contradictory/ambiguous issues that may arise in connection with the present KYC procedure. That means, that in case of discrepancies between this KYC procedure and the Estonian legislation, the Compliance executive / responsible person(s) shall act in accordance with the Estonian legislation, as prevailing.

COMPANY SANCTIONS COMPLIANCE POLICY

Annex 1 to the KYC Policy

Company Sanctions Compliance Policy constitutes an integral part of the general KYC policy and entitles responsible persons, employees, managers, the Company's officials to act in accordance with Sections 3 and 4 of the KYC policy.

This Annex applies to hProof and its wholly owned subsidiaries and must be adopted by its direct and indirect controlled entities in Estonia and in other countries, always in compliance with these entities' documents of incorporation and applicable laws. Adoption of the KYC policy is encouraged in other entities in which hProof has an indirect participation interest in Estonia and in other countries.

All contractors/employees and Executives of hProof and its controlled entities must be committed and abide by the rules established in the KYC policy, specifically with the sections connected with observing the international and local Sanction regulations, specified in Sections 3 and 4 of the KYC procedure. The Executives and/or responsible persons are responsible for disseminating these Policies among the employees/contractors of the Company, by providing necessary training and monitor that all employees/contractors, followed the guidelines contained herein,

All Providers, including other Partners of hProof, must know and observe this Company Sanctions Compliance Policy in order to guide their conduct and avoid conflicts and violations. The access to the Policies both the KYC and Sanctions Compliance Policies may be provided to the Clients upon request.

The guidelines established in these Policies must be applied globally, even if the respective local legislation has more lenient rules and accepts and/or tolerates some conducts provided for herein. In case of the conflict of laws, such conflict shall be reported to the Responsible person, specially appointed to monitor the implementation of the KYC and Company Sanctions Compliance Policies.

hProof will commit all necessary measures to ensure proper Company Sanctions Compliance Policy procedures and its implementation in the Company’s day-to-day activity, in accordance with both local and international regulations in regard to the Sanctions Compliance Policy.