RFT Exhibit 3

DETAILED CONTRACT SPECIFICATION

"Lease of Hardware with Software, necessary for providing security services for OSE"

Procedure ref. ZZ.2131.218.2018.TKI[OSE2018]

Table of contents

I. Definitions

For the purposes of interpreting the provisions of the Agreement and the requirements specified in DCS, the Parties stipulate the following meaning of the corresponding terms:

1)	**System Update**	An element of the Planned Works submitted by the Contractor, to the Awarding Entity, the purpose of which is to update the elements of the System;
2)	**Failure**	Every case of irregular operation of the System, regardless whether it occurred for a reason for which the Contractor is responsible. The occurring Failure authorises the Awarding Entity to make a Request. Failures shall not include administrative and servicing activities performed in the System by the Contractor or the Awarding Entity.
3)	**Critical Error**	System operation not compliant with the specification defined in chapter IV. Detailed requirements affecting the scope and quality of System operation, resulting in Failure preventing the performance of at least one of the key functions (in particular such as: Internet access, web traffic filtering, SSL control, ensuring the availability of the management console for administrators) by the System to all or most users of these functions, as well as preventing the performance of the key functionalities implemented by the System, regardless of the number of users affected by such irregularity. Critical Errors also include degraded System efficiency that impacts all or a significant share of users. Failure of Hardware and its modules as a result of which the System loses its redundancy is also a Critical Error.
4)	**Non-Critical Error**	System operation not compliant with the specification defined in chapter IV. Detailed requirements affecting the scope and the quality of the System's operation and leading to a Failure which disturbs the performance of the System's functions or disabling such functions for individual users. Any degradation of System performance that affects individual users is also considered Non-Critical Error;
5)	**Error / System Error**	The reason for the Failure to be removed by the Contractor under the Agreement. System Errors include Critical Errors, Non-Critical Errors and Faults;

6)	**Total Price**	The total price, including taxes, fees and other public law charges, included in the Contractor's offer for the performance of the subject of the Agreement;
7)	**Repair Time**	The time which elapses from the moment the Contractor submits the Request to the moment of the Repair;
8)	**Time to restore System – use of the Workaround**	The time which elapses from the moment of submitting the Request to the Contractor to the moment of applying the Workaround
9)	**Response Time**	The time which elapses from the moment of submitting the Request to the Contractor to the moment the acceptance of the Request for processing is confirmed;
10)	**Documentation**	The documentation containing the technical concept of the System implementation at the Awarding Entity's server room, to be prepared by the Contractor within 5 Business Days after signing the Agreement, and the post-implementation documentation to be prepared by the Contractor prior to System Acceptance, including any changes and modifications thereto developed as part of the implementation of the Agreement;
11)	**Business Day**	Any Every day from Monday to Friday, except for the statutory free public holidays in Poland;
12)	**Physical Access**	Activities performed by the Contractor under the Agreement at the location of the System;
13)	**Working Hour**	Any full clock hour between 8 A.M. and 5 P.M. on a Business Day;
14)	**Project Manager**	A person acting on behalf of the Party appointing it (by the Awarding Entity and the Contractor, respectively) whose task is to supervise the performance of the Agreement and to exercise other permissions and obligations specified in the Agreement;

15)	**Consortium**	The Contractors undertaking jointly the performance of the subject of the Agreement and whose mutual relations are governed by a consortium agreement or other agreement of a similar nature, especially a cooperation contract.
16)	**Repair**	Restoration of the System's functioning by removing Errors and restoration of its operationality in accordance with operational parameters, specification, documentation or other arrangements (if any) between the Parties. The Repair will be considered successful upon its verification and confirmation by the Awarding Entity's Project Manager;
17)	**NASK**	Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy, with the registered office in Warsaw;
18)	**Workaround**	Restoration of the System's functioning by removing Errors and restoration of its operationality in accordance with relevant arrangements made between the Project Managers of both Parties, which, however, is not considered normal operation of such functionality, or which causes the System to operate below expectations resulting from its specification. The Workaround is not considered a Repair. The Workaround allows to carry out all processes related to the proper operation of the System however, it requires additional actions from users or causes the System to operate below the requirements specified in the operational parameters. The Workaround can be also a modification of the course of a System process if approved by the Awarding Entity's Project Manager;
19)	**System Acceptance**	Confirmation of the Contractor's completion of System Stage 1 in line with the Agreement and the Documentation;
20)	**System Expansion Acceptance**	Confirmation of the Contractor's completion of System Stage 2 in line with the Agreement and the Documentation;
21)	**Tender**	A written statement submitted by the Contractor regarding the performance of the subject of the Contract, in accordance with the provisions of the Request for Tender, submitted to the Awarding Entity as part of the public procurement procedure leading to the conclusion of the Agreement;

22)	**Software**	The software integrated with the Hardware and ensuring the functionalities defined in DCS;
23)	**OSE Network**	The Nationwide Educational Network called OSE (Ogólnopolska Sieć Edukacyjna) which is referred to in the Polish Act (27 October 2017) on the Nationwide Educational Network (Polish Official Journal: Dz. U. 2017. 2184);
24)	**Planned Works**	The works of which the Contractor notifies the Awarding Entity 3 Business Days in advance, with their scope and duration to be approved by the Awarding Entity, whose purpose is System maintenance and Updates. Such works can cause an interruption in the access to the entire System (System will not be available or perform its functions during the execution of such works) or any part thereof (the System will allow for limited operation, for example without web traffic filtering or SSL traffic control, console log-in functionality). Planned Works can be carried out only outside Working Hours;
25)	**Employees**	Persons employed by the respective Parties or their associated entities (as referred to in Article 4.1.5 of "Commercial Companies Code" of 15 September 2000) and others whom the Parties or their associated entities hire based on agreements other than employment contract.
26)	**Priority**	status assigned to a Request and used to define Response Time and Repair Time;
27)	**Reinstallation**	Repeated installation of the Software on the Hardware specified by the User;
28)	**Relocation**	Transfer of the System from the original data processing centre in Warsaw to another data processing facility in Warsaw (to be specified by the Awarding Entity), by the Contractor upon the Awarding Entity's request. Only one Relocation will take place during the effective term of the Agreement. The Relocation will be carried out outside Working Hours;
29)	**Force Majeure**	An extraordinary event or circumstances beyond the reasonable control of the Contractor or the Awarding Entity , which cannot be reasonably prevented before the date of conclusion of the Agreement, whose occurrence cannot be reasonably avoided or overcome, and which essentially cannot be attributed to either the Contractor or the Awarding Entity;

30)	**DCS**	The Detailed Contract Specification enclosed in RFT Exhibit 3;
31)	**System**	The Software installed on the Hardware at the data processing centre specified by the Awarding Entity;
32)	**Agreement**	This Agreement concerning public procurement (Lease of Hardware with Software Necessary for providing security services for OSE) related to the responsibilities of a public telecommunications network operator which have been imposed on the Awarding Entity by means of the act of the 27 October 2017 on the Nationwide Educational Network (OSE Network);
33)	**Hardware**	The Contractor's devices which the Contractor delivers to the data processing centre specified by the Awarding Entity and lends for use by the Awarding Entity, including Software installed on the Hardware and constituting the System;
34)	**Instructional Service**	Training for System users and administrators of the Awarding Entity. Successful completion of the Instructional service will be confirmed in the System Acceptance certificate;
35)	**Support Service**	The Contractor's handling of the Awarding Entity's Requests aimed at the Repair of System Errors and Faults;
36)	**Technical Assistance Service**	consulting services and additional works provided by the Contractor with regard to System operation;
37)	**System Implementation**	Supply, installation, integration and commissioning of the System at the data processing centre specified by the Awarding Entity, including delivery of the Documentation and System configuration according to the Awarding Entity's guidelines. The successful completion of the System Implementation will be confirmed in the System Acceptance certificate. The detailed description of System Implementation is provided in chapter IV. Detailed requirements point ;
38)	**Services**	The following services: Support, Instructional and Technical Assistance;

39)	**Fault**	The System does not operate in compliance operation which is not compliant with the specification referred to in chapter IV. Detailed requirements – it impacts affecting the extent scope and the quality of the System's operation and leadings to inconvenience during the use of the System without limiting the execution performance of the System's functions but disturbing disrupting the work of its users;
40)	**Manufacturer's Technical Support**	Technical support package purchased by the Contractor from the manufacturer including a System for reporting Errors and Faults.
41)	**Exhibit**	An appendix to the Agreement:
42)	**Request**	A request submitted to the Contractor concerning an occurring Failure;
43)	**RFT**	The Request for Tenders;

II. General Principles

The contract includes the lease of the System for the purpose of protecting users against dangerous web content by applying web content filtering solutions as required for the use and provision of security services in OSE Network.

Within the framework of the contract, the Contractor will supply also the following services: Instructional, Support, Technical Assistance.
Upon a request of the Awarding Entity, the Contractor may be required to Relocate the System once during the effective term of the Agreement.

All requirements and parameters (including technical, functional and efficiency related) specified in DCS are compulsory for the Contractor and it is obliged to meet them within the proposed System price.

At the end of the System lease and thereafter, the Awarding Entity intends to launch the final system for user protection against dangerous content. According to OSE Network guidelines, the final system will be scaled up to 30,000 schools. The Awarding Entity plans to initiate a procurement procedure concerning the final system for OSE Network in 4Q 2018 or 1Q 2019. The Awarding Entity assumes that the conditions and method for selecting the final system will be similar to those of the current procurement procedure, however the final system will be purchased and not leased.

III. Timetable for the performance of the subject of the Agreement

1) Stage 1 to be implemented within 24 days of the date of conclusion of the Agreement;
    a. System Implementation in the scope required to support 2,400 schools (72,000 workstations; 12,000 HTTP/HTTPS requests per second) and 20 Gbps of Internet traffic, with full control (SSL decryption and encryption) of the encrypted traffic going through the Hardware;
    b. Instructional Services.

2) Stage 2 to be implemented within 24 days of the Contractor receiving the System expansion request:
    a. expansion of the System as required to support 4,400 schools (132,000 workstations; 22,000 HTTP/HTTPS requests per second) and 36 Gbps of Internet traffic, with full control (SSL decryption and encryption) of the encrypted traffic going through the Hardware; Documentation update.

3) Support and the Technical Assistance Services throughout the entire effective term of the Agreement;

The Awarding Entity is required to order the implementation of Stage 2 from the Contractor, however the time of the order will be at the sole discretion of the Awarding Entity. Therefore, Stage 2 will be implemented only if the Awarding Entity submits to the Contractor express written request to do so.

The System will be implemented at the data processing centre in Warsaw specified by the Awarding Entity, on the Hardware to be supplied by the Contractor. The Awarding Entity may change the place of the System's implementation (Relocation) once during the effective term of the Agreement.

IV. Detailed requirements The following are the detailed requirements applicable to the respective System modules. The Contractor must meet the requirements defined in Stage 1 within the proposed price of that Stage. The System will be capable of supporting full traffic volume specified in chapter **Błąd! Nie można odnaleźć źródła odwołania.** for the given Stage.

1. Common requirements for all System elements

1) The System will support IPv4 and IPv6 both in terms of traffic analysis and the management system.
2) The Awarding Entity is in possession of two 24-port network switches: Cisco Catalyst 4500X24X-IPB supporting WCCP v2 (GRE/L2). The Awarding Entity will provide 16 ports (10 GE) on each switch for the Contractor's use. During the installation of the System, the Contractor will connect each Hardware item to both switches and configure LACP on such Hardware to aggregate the traffic management interfaces of both switches. If the supplied Hardware requires more traffic ports, the Contractor will deliver appropriate switching Hardware within the Stage 1 price.
3) The Awarding Entity must be able to manage the System using CLI and a Web GUI console available in a web browser (TLS secured).
4) The Contractor will assemble the Hardware in a 19” rack and supply all assembly kits at its own expense.
5) The System will have integrated diagnostic tools (at least ping and traceroute).
6) The Hardware will be fitted with a redundant AC power supply.
7) The Contractor will supply cabling to connect the Hardware and the System to the Awarding Entity’s network, according to technical parameters. Servers will be supplied with power cables and network cables (SFP+) compatible with the switches specified in point 2. The Contractor will deliver SFP+ modules for each of the switches and two SFP+ modules for each of the supplied servers, or SFP+ DAC cables (3 metres long) – the switch and servers will be fitted into one rack. The network cables and the modules will be compatible with Cisco Catalyst 4500X24X-IPB.
8) The Contractor will secure access to all System elements by means of password protection. All log-in data will be provided to the Awarding Entity during the System Acceptance procedure.

9) The System will ensure High Availability (HA) for its key services (especially: Internet access, web traffic filtering, SSL control, management console availability). The System will have integrated load balancing mechanisms and allow the use of external load balancers. The Awarding Entity will provide two network switches supporting WCCP v2 (GRE/L2). If the Contractor chooses to use it in a HA environment, it will provide the configuration procedure for such switches. If the Contractor chooses to use other load balancing mechanisms to build the HA environment, it will supply all necessary hardware and licencing for the Stage 1 price.
10) The Contractor will ensure the availability of the Manufacturer's Technical Support for the System throughout the entire effective term of the Agreement.

2. Web content filtering module

1) The manufacturer of the Software must be a member of Internet Watch Foundation (IWF) or another organisation of similar status and reach.
2) The System must support Internet Watch Foundation (IWF) or equivalent databases for filtering and reporting purposes. The System must block CSAM-child sexual abuse materials by actively implementing IWF's CAIS list (Child Abuse Image Content URL list) or equivalent lists.
3) The System must feature *forward proxy* in *explicit* and *transparent* versions for the entire traffic.
4) For the *transparent* mode, the System will support all of the following for the entire traffic:
    a. *inline*
    b. WCCP v2 (GRE/L2) redirection
    c. Policy Based Routing.
5) For *proxy* mode, the System must support the following protocols: HTTP, HTTPS. For other protocols, traffic passthrough function must be available.
6) The System must allow the Awarding Entity to freely create at least 50 web filtering policies, i.e. a set of rules defining:
    a. HTTP, HTTPS traffic filtering based on a specialist database (referred to point 8) and own database of categories (referred to in point 14.a), including support for exceptions based on own database of categories (referred to in point 14.b), in particular white- and blacklists. The exceptions must be based on a defined range of IP addresses, i.e. the given non-filtered category will be applicable to subnet A but not subnet B.
    b. processing of encrypted traffic exceptions (SSL Proxy) – SSL decryption will be excluded based on a specialist database (referred to in point 8), specifically for the following categories: banking & finance, healthcare, e-mail, and own database of categories (referred to in point 14.c);
    c. anti-virus analysis – enabling/disabling (according to points 29 – 32);
    d. application control – enabling/disabling (according to point 36).

7) The System must enable activation of specific filtering policies (referred to above) for specific IP address ranges, but not less than 4400 (the number of schools in Stage 2), and for user groups which will be defined locally (according to point 20), or based on an external identity system or external user repositories (at least LDAP, RADIUS).
8) The System must filter HTTP/HTTPS traffic by comparing webpage requests and IP address with a specialist database (to be supplied by the Software manufacturer), divided into webpage categories ("Webpage Categorisation") and contain information about domains, URLs.-
9) The specialist database (point 8) must have at least 50 content categories, including specifically the categories referred to in point 35, which the Awarding Entity must be able to use in any way to create filtering policies.
10) For the unknown-category webpages and pages marked by the Awarding Entity included in the database referred to in point 14.a and the specialist database referred to in point 8, the Content Categorisation process must be performed in real time (Dynamic Content Analysis). Traffic latency for Dynamic Content Analysis must not exceed 250 ms per page. The System will enable the Awarding Entity to mark categories (referred to in point 9) to redirect queries to Dynamic Content Analysis, but not more than 15 categories (including specifically the categories listed in point 35.e). The results of Dynamic Content Analysis must be allocated higher priority than results of the static analysis which uses the databases (point 8).
11) Dynamic Content Analysis must be based on lexical analysis or dynamic Machine Learning/AI mechanisms. Dynamic Content Analysis must not be Regex based only. The Contractor must provide options for the Awarding Entity to further develop the Dynamic Content Analysis mechanism, specifically by new vocabulary definitions or Machine Learning algorithm training. During Stage 1, upon request by the Awarding Entity, the Contractor must extend Dynamic Content Analysis options to include recognition of up to 3 new pieces of content in Polish or English.
12) Dynamic Content Analysis must analyse content in Polish and English.
13) The Contractor must provide options for the Awarding Entity to adjust the sensitivity of the Dynamic Content Analysis mechanism based on a threshold which, if exceeded, will block/pass certain webpages. If the threshold needs to be adjusted, the Awarding Entity will request it from the Contractor. Such requests must not be included in the working time available under Technical Assistance and cannot be submitted more than once every 4 weeks.
14) The Awarding Entity must be able to create its own custom database of categories including:
    a. at least 10 new categories defined by the Awarding Entity and including issued other than those found in the database referred to in point 8;
    b. at least 4,400 categories (a list of URL addresses) to be used for exception handling based on user submissions to the filtering policy (black- and whitelists);
    c. at least 2 categories (a list of URL addresses) to be used for exception handling in SSL decryption policy.

    The System must enable periodic import of the custom database from external repositories as needed for the filtering policies.

The System must feature an access control mechanism for such database, including user activity logging and version control.

15) The specialist database referred to in point 8 must be continuously updated by the Software manufacturer, by each time applying at least the following mechanisms:
    a. Internet resource browsing and analysis mechanisms;
    b. advanced mechanisms for page content classification based on at least machine learning and lexical analysis;
    c. a team of people to verify the correctness of classification.

    However, the mechanisms mentioned in points b and c must analyse webpage content based on the published text, including its context, images and videos (and their content), links and their reputation.
16) The specialist database referred to in point 8 must contain "Uncategorized" category for use by the Awarding Entity in the filtering policy when Dynamic Content Analysis cannot assign any category to a webpage.
17) If the System identifies a violation of the filtering policy and logs a webpage that should be blocked, the System must provide options for the Awarding Entity to define at least all of the following actions to be executed by the System for the given user:
    a. block access to a webpage;
    b. display a pre-entry warning to the user, with an option to enter the page after reading the warning;
    c. display of an “access-blocked” page with log-in fields for the user to authenticate the current session (mechanisms described in point 20) and temporarily override the filtering policy (cookie override);
    d. redirect of the user to an external user authentication portal.

    The System must enable the Awarding Entity to assign the actions referred to in items a – d to specific categories or lists thereof (for example, if a webpage requested by a user is categorised as "Drugs", it will always initiate action "A", and in the case of "Alcohol" -always action "D").
18) The process of category classification must include evaluation of webpage reputation based on a graded trust scale and score assigned to the given page.
19) The System must enable the Awarding Entity to block TOR access, even in the case of *pluggable transport protocol.*
20) The System must provide a user and administrator authentication process based on local database and protocols: LDAP, Kerberos and RADIUS.
21) The System must enable the Awarding Entity to define policies for unidentified users.
22) The System must enable the Awarding Entity to define various administrator roles, including different levels of administrator rights. In particular, the System must enable administrator access in read-only mode (all configuration options visible for monitoring purposes only).
23) The system must provide:

a. HTTPS traffic decryption based on TLS, version 1.0 or higher (at least RSA and DH and ECDHE);
b. selective activation of the decryption function to bypass certain categories defined by the Awarding Entity in the filtering policy (referred to in point 6.c);
c. definitions of decryption exceptions in encrypted traffic based on URL/subnet, URL categories.

24) When decrypting HTTPS traffic, the System must provide server certificate control for servers accessed by users (checking at least the validity and certification chain). If the certificate is invalid, the System must be able to block the current session.
25) When decrypting HTTPS traffic, the System must not use different sets of encryption algorithms in client and server communication, specifically the client cannot use a worse encryption mechanism than the server.
26) The System must block encrypted pages after analysing server certificate, for example by blocking of the domain and subdomains lacking TLS decryption, even if the decryption mechanism is deactivated or TLS decryption is not able to decipher the given page.
27) When decrypting an encrypted string, the System must tunnel traffic without modification or perform only validation of encryption certificates described in point 24.
28) The System must enable the Awarding Entity to detect and block tunnelling in HTTP/HTTPS protocols (with option to enable/disable), for example SSH session blocking on port 443.
29) The System must enable the Awarding Entity to scan files (sent and received by users through the System) with anti-virus/anti-malware scanners with periodic definition database updates performed several times per day. In particular, the System must scan for viruses in files which are sent through e-mail and downloaded from the Internet.
30) The System must enable blocking of certain file types to be specified by the Awarding Entity, based on their extensions and MIME, for example executable files, PDF files, images, compressed files, etc., and files which cannot be scanned by the anti-virus engine (because of their encryption method, for example).
31) The System must enable configuration of notifications with custom text to be displayed when a virus is identified.
32) The System must ensure that definition databases are updated with configurable frequency. During the update process, the functionality must not be compromised, and if an update is unsuccessful, the previous definitions must continue to be applied.
33) The System must enable the Awarding Entity to use the full functionality of Safe Search in search engines (at least Google, Youtube, Bing).as provided by its supplier.
34) The System must enable webpage filtering based on at least 20 defined phrases to be specified by the Awarding Entity, such as "legal boosters", "twitter porn", "blue whale game".

35) The System must enable recognition of content concerning at least the issues listed below. The System must enable the use of recognised content in the development of the category-based filtering policy. The Contractor must implement a System where all of the following types of content are recognised, and aggregated into at least four separate categories (types A, B, C and D):

a. Type A content category:

- content defined in Polish law as prohibited from publication or public exposure, including:
  i. content showing pornography with minors, also referred to as CSAM (child sexual abuse materials);
  ii. content showing paedophilic materials, their dissemination and advocating;
  iii. content showing online seduction of minors;
  iv. content showing public promotion of fascist or other totalitarian regimes, incitement to hatred towards differences based on nationality, ethnicity, race, beliefs or lack thereof;
  v. content showing publicly distributed and exposed information which may facilitate unlawful terrorist activity;
  vi. content showing public insulting of a group or an individual based on their nationality, ethnicity, race, beliefs or lack thereof;
  vii. content showing information about illegal drugs, legal boosters – websites discussing, encouraging, promoting, offering, selling, delivering or otherwise advocating the use, cultivation, production or distribution of illegal drugs and legal boosters (including non-pharmaceutical drugs, intoxicating plants, chemical solvents or other chemicals), as well as accessories associated therewith;
  viii. pages used to offer gambling games against the gambling law*.
- pornography – pages showing pornographic content, such as text, image or video with a graphic depiction of a person or an object of explicitly sexual nature;
- violence – pages intended to show physical injury or other damage caused to people, animals or property, or to provide instructions how to cause such injury or damage;
- adults only – pages showing materials intended for adult audience but not classified as pornography or violence. Such pages often contain vulgar, erotic or other content not appropriate for children;
- alcohol and tobacco – pages and materials promoting alcohol and tobacco, the sale and use thereof, for example beer, wine and strong alcoholic beverages;

- weapons and explosives – pages and materials promoting weapons, their manufacturing, use and customisation, for example pistols, rifles and explosive materials;
- anorexia and other eating disorders – pages and materials promoting unhealthy and improper lifestyle involving eating disorders;
- self-mutilation – pages and materials promoting dangerous, unhealthy and improper lifestyle involving wilful injury of one's own body inflicted by self-aggression or depression;
- content showing psychomanipulation, i.e. controlling the emotions of other persons for the purpose of fraud or incitement towards improper (often risky) behaviour.

b. Type B content category:

- illegal software or other unlawful content – pages which illegally make available copyrighted software or other materials (for example, music, films), or which provide information about the sourcing of such materials (for example, peer-to-peer technology);
- online gaming – pages which provide access to online games (except for games used for educational purposes);
- swearing – pages and materials showing content intended to expose words and expressions commonly recognised as indecent, obscene and vulgar;
- online betting – pages not recorded in the official Register of Illegal Gambling Domains and where users can bet or participate in betting, lotteries or receive related information, support, instructions or training*;
- dating portals – pages intended to facilitate encounters between people for matrimonial or mating purposes and information exchange for virtual/physical date arrangements intended to establish lasting or short-term relationship (often exclusively of sexual nature);
- online chat – pages or software enabling online chatting, voice communication, video conferences;
- varied adult content – pages showing adults-only content not classified into a separate category;
- vandalism and violence – pages and materials showing content intended to promote the violation of legal order, acts of vandalism, football hooligan activity (for example, promotion of violent behaviour, etc.).

Also, for research and development purposes, in a limited test environment, the Contractor will propose filtering solutions for the following types of content:

c. Type C content category:
   - psycho-manipulation groups – pages promoting and providing information about psycho-manipulation quasi-religious groups;
   - health and life hazards – content promoting, selling, advocating or discussing body modification, such as tattoos, piercing and other behaviours dangerous to the life and health of minors;

d. Type D content category:
   - uncategorized / none – pages outside the Contractor's database or considered ambiguous by the Contractor's Categorisation engines;
   - social media, blogs and information exchange sites involving harmful and illegal content;
   - pages offering file uploading, storage and sharing;
   - pages providing product/service shopping solutions (for example Internet auction portals, online shops) involving harmful and illegal offerings.

* – as "pages used to offer gambling games against the gambling law" (Type A) and "online gambling" (Type B) must be filtered separately, the Contractor must ensure such separated treatment based on a URL list (blacklist) – the Contractor must prepare such list for "pages used to offer gambling games against the gambling law" category. The list must be compliant with the Register of Illegal Gambling Domains, as published on the Ministry of Finance website (). The blacklist update process is exempted from the requirements of point 15.

NOTICE: The above content classification is stated here and in the procurement procedure ONLY for the purpose of conducting the procurement procedure – the System selected during the procedure will only enable the recognition of various types of content and user security. The selection of specific categories depends on the respective school headmasters. Note that the user protection system must not limit pages related to banking & finance, healthcare and e-mail.

36) The System must enable the Awarding Entity to limit certain functionality of social media portals by choosing which functions will be accessible, and ability to block web apps (both desktop and mobile platforms) of the following type:

a. instant messaging;
b. web anonymisers;
c. web tunneling;
d. peer to peer;
e. photo/video sharing;
f. adult multimedia.

37) The System must enable the Awarding Entity to block access to numeric hosts (option to enable/disable).
38) The System must record logs containing at least the following information:
    a. Transaction date (local time);
    b. source IP address;
    c. Username (if authenticated);
    d. URL category;
    e. Target IP address;
    f. Full URL string;
    g. Hostname/subject from the certificate;
    h. Searched expressions;
    i. Encrypted connection status (decrypted or not).
39) For integration with the Awarding Entity's systems, the System must support the following functionalities:
    a. VLAN;
    b. LACP;
    c. Routing.
40) The System must enable the Awarding Entity to customise error messages and general notifications displayed to users (for example, the “access blocked” page), specifically session-related information:
    a. authenticated username;
    b. error text;
    c. source IP address;
    d. reason to block access (category name, dynamic classification mechanism activated to block the page);

e. IP address or name of the blocking device.

41) The System must enable sending of Awarding Entity's customised notifications about the System's operation (via SMTP).

42) For load control, the System must enable communication of at least the following information (via SNMP) to the Awarding Entity's systems:

a. CPU – Idle time,
b. CPU – Percentage spent on processes in the user space;
c. CPU – Percentage spent on process in the system space;
d. Memory – Total Free;
e. Memory – Total Real;
f. Memory – Avail. Swap;
g. Storage – disk usage.

3. Management Module

1) The System must have a graphical tool for the development of filtering policy with functionalities for building/adjusting filtering polices based on flat file changes or REST API.
2) The System management console for administrators must be included with the System delivered to the Awarding Entity and accessible to the Awarding Entity via graphical interface (local or central console) as well as via the command line.
3) The System must enable the Awarding Entity to manage administrator access to the console based on assigned roles, including Awarding Entity's definitions of own roles.
4) The System must provide access to the graphical interface of the console through a secure encrypted connection.
5) The System management console will enable the Awarding Entity to execute all functionalities related to management and implement all privileges.

4. Reporting Module

1) The System must have at least 10 pre-defined reports and options for the Awarding Entity to add at least 10 custom reports.
2) The System must enable the Awarding Entity to archive Access Logs after a period defined by the Awarding Entity (for example, 30 days).
3) The System must enable the Awarding Entity to anonymise certain fields in reports (at least user IP and username).

4) The System must have a reporting tool for manual and automated generation of reports showing all parameters monitored and controlled by the System. In particular, the reporting tool must generate reports on outgoing traffic to specific external IP addresses, websites and their elements, and traffic of specific internal users or IP addresses. In particular, the System must enable the Awarding Entity to generate reports showing at least:
    a. TOP 10 categories: permitted, passed, according to the filtering policy;
    b. TOP 10 categories: banned, blocked, according to the filtering policy;
    c. TOP 10 popular web apps;
    d. TOP 10 popular web pages;
    e. TOP 20 blocked web pages;
5) The System must have options for exporting reports at least in PDF format.

5. System Implementation

1) Supply, installation, integration and commissioning of the System in the data processing centre, including configuration on the network level.
2) System integration with the user/administrator repository delivered by the Awarding Entity (LDAP).
3) Configuration of two filtering policies with different filter levels, based on the Awarding Entity's guidelines.
4) Configuration of 2 custom report templates, based on the Awarding Entity's guidelines.
5) Preparation of the System Implementation technical concept for the data processing centre specified by the Awarding Entity, including least the following information:
    a. System requirements regarding infrastructure, including:
        – required number of units in the Awarding Entity's rack;
        – power consumption (kW) of the System.
    b. the method of connecting the System to the Awarding Entity's network, including:
        – a logical diagram showing:
            - the method of connecting the Hardware to the Awarding Entity's network;
            - the structure of connections between the Hardware units supplied for System development purposes.
        – a description of services available in the respective Hardware units.

c. System testing plan, according to the System Acceptance criteria, including:
   - Test plan ID;
   - Description of the test subject ;Test range - tested properties;
   - Test exclusions;
   - Testing approach;
   - Test pass/fail criteria;
   - Test stop/re-run criteria;
   - Deliverables;
   - Testing actions and tasks;
   - Test environments;
   - Roles and responsibilities;
   - Resource requirements ;
   - Test timetable;
   - Risks and contingency plans.

d. requirements regarding the hardware to be supplied by the Awarding Entity as necessary for the Instructional Services;
e. Cisco Catalyst 4500X24X-IPB switch configuration procedure for initiating WCCPv2 (GRE/L2) and redirecting network traffic to the Hardware;
f. list of Hardware installed in the data processing centre with at least the following information for each Hardware unit:
   f.i. Serial number;
   f.ii. Value.
g. procedures for effective data erasure from the Hardware drives before the Hardware is uninstalled from the Awarding Entity's data processing centre after the expiry of the Agreement;
h. a template of a Request e-mail for the purposes of performing Support Services by the Contractor, defining details to be included therein.

The Awarding Entity's approval of the System Implementation technical concept shall not exempt the Contractor from the obligation to meet all requirements under DCS.

6) Preparation of post-implementation documentation in Polish or English, including at least:
    a. A physical diagram showing the method of connecting the Hardware to the Awarding Entity's network, including names of the connected Hardware units, the number and types of network interfaces;
    b. A logical diagram showing the method of connecting the Hardware to the Awarding Entity's network, including a description of the System elements or functionalities performed by individual Hardware units;
    c. Connection mapping for the respective System elements;
    d. The initial configuration of all System elements at the time of handing over the System to the Awarding Entity;
    e. A table with IP and MAC addresses of the respective Hardware units;
    f. A technical specification of all supplied System elements;
    g. System operation procedures for the following activities:
        – Log-in procedure for all System elements;
        – Adding new users;
        – Password resetting by individual users;
        – Adding and editing filtering policies;
        – Adding and editing the Awarding Entity's category database for each school;
        – Configuration of school-level filtering exceptions, based on IP addresses;
        – Adding new reports;
        – Monitoring the correctness of System operation;
        – Installation of system patches;
        – Creating backup copies of configuration and other data;
        – Generating certificates used in SSL traffic decryption/encryption;
        – Adding certificates to Trusted Root CA for various operating systems, specifically Apple (macOS, OS X), Windows (XP and later) and Linux (Debian, Ubuntu, CentOS), as well as web browsers with own certificate systems (specifically Firefox).
7) Development of scripts for adding Awarding Entity's certificates to Trusted Root CA for operating systems and web browsers with own certificate systems (specifically Firefox). Such scripts must be executable on Windows (Win 7 – Win 10), Linux (Debian, Ubuntu, CentOS), Apple (macOS, OS X) operating systems.

8) Development of the “access blocked” page (displayed to a user when access to the given page becomes blocked based on the filtering policy), according to the Awarding Entity's guidelines – a static page in html with fields for entering the log-in information for policy override.
9) The Contractor must provide storage space in the Hardware for the purposes of storing Access Logs for the period of 3 months, as well as two custom reports defined by the Awarding Entity covering a selected range of IP addresses and the last 30 days.
10) The Contractor must support the Awarding Entity during the System's integration with its Fault Management system (ZABIX) – at least the following data must be transmitted via SNMP:
    a. CPU – Idle time,
    b. CPU – Percentage spent on processes in the user space;
    c. CPU – Percentage spent on process in the system space;
    d. Memory – Total Free;
    e. Memory – Total Real;
    f. Memory – Avail. Swap;
    g. Storage – disk usage.
    h. The service will be tested by:
        – Sending HTTP GET to and checking whether the “access blocked” page will appear;
        – Sending HTTP GET to and checking the certificate used to sign the page. The certificate parameters need to match the certificate imported to SWG.

In order to duly perform the contract (especially Support and Technical Assistance Services) and the Planned Works, the Awarding Entity must provide remote access to the System for the authorised representatives of the Contractor. The Contractor must create and use individual administrator accounts in the System. The Contractor guarantees that, within the framework of the Support and Technical Assistance Services the Contractor will use the System only for the purposes of performing requested tasks or Repairs, and in particular the Contractor will install previously tested solutions in the System.

6. System Relocation

Upon request from the Awarding Entity, the Contractor may be required to Relocate the System once during the effective term of the Agreement. The Awarding Entity must serve such request at least within 30 days before the arranged System Relocation date. The Contractor will confirm the receipt of the request and start its execution on a date agreed with the Awarding Entity. The Relocation will be assisted by the Awarding Entity.

The Contractor shall assume full responsibility for the Hardware during the Relocation process, from the disconnection of the Hardware from the Awarding Entity's network to its re-connection at the new data processing centre.

The Relocation must be carried out outside Working Hours and must not be longer than 2 days. The Relocation time is counted from the deactivation of the System to its restoration, confirmed by tests referred to above.

Once the Hardware is installed at the new data processing centre and connected to the Awarding Entity's telecommunications network, the Contractor will conduct tests based on test scenarios implemented at the System Acceptance stage, in order to confirm the correct operation of the System at the new location.

7. Technical Assistance Service

The Technical Assistance Service involves consulting as well as the performance of additional works related to the System's operation, throughout the effective term of the Agreement, but not exceeding a 160 hour package of such services and works. The Technical Assistance Service will be provided based on time limits assigned to Priority 3 Requests. The Technical Assistance tasks will be ordered from the Contractor by the Awarding Entity's Project Manager, via e-mail, including details regarding the scope, deliverables expected by the Awarding Entity and the time limit. In response to the received order, the Contractor will provide the Awarding Entity with information about the estimated workload of the ordered Technical Assistance tasks and viable time frames. The Contractor will start performing the Technical Assistance Services once the Awarding Entity accepts the estimated workload and time frames. After the completion of the Technical Assistance tasks, the Parties will draw up an acceptance certificate, including information about the number of working hours used while performing the Service.

The Awarding Entity may specify another method for submission and processing of Technical Assistance requests, in particular by providing the Contractor with access to a specific system used by the Awarding Entity.

The Technical Assistance Service may involve the following in particular:

a. System reconfiguration;
b. integration with the Awarding Entity’s other systems;
c. initiation of new System functionalities, based on the Awarding Entity's guidelines;

d. tasks related to System expansion.

8. Support Service

The Support Service involves the processing of Requests submitted by the Awarding Entity's assigned employees to the Contractor with the use of the agreed method. When processing a Request, the Contractor will perform diagnostics by analysing causes and circumstances of the given Failure, specifically in terms of any System Errors, and will make Workarounds and Repairs. The results of such works will be delivered to the Awarding Entity. During the diagnostics stage, the Contractor's team shall be authorised to contact the Awarding Entity via e-mail or telephone to obtain additional information..

Requests will be submitted by telephone or e-mail to the specified Contractor's address, with telephone submissions to be confirmed afterwards also by e-mail. Requests related to Critical Errors will be confirmed by the Awarding Entity's Project Manager. The Awarding Entity may define another method for submitting and processing Requests, in particular by providing the Contractor with access to a specific system used by the Awarding Entity.

The Contractor will provide Support Service 24/7 – 24 hours a day, Monday - Sunday, during the entire effective term of the Agreement.

Request Priorities:

1 Critical Error – symptoms imply that a Critical Error occurred in the system;
2 Non-Critical Error – symptoms imply that a Non-Critical Error occurred in the system;
3 FailureFault – symptoms imply that a Fault occurred in the system.

Priority will be assigned to Requests by the Awarding Entity.
When verifying a Request for completeness, , the Contractor may ask the Awarding Entity's Project Manager to decrease its Priority. The Awarding Entity's Project Manager will notify the Contractor about such lower Priority assignment, or it will reject the Contractor’s request.

The implementation of a Workaround accepted by the Awarding Entity will automatically cause a lower Priority to be assigned to the given Request.

As a result of the diagnostics stage, the Contractor's team shall be obliged to:

a. if it is established that the Request was caused by a System Error – confirm the priority (priority 1 – critical error; priority 2 – non-critical error; priority 3 – Fault) and initiate the Repair process using the Contractor's resources or the Manufacturer's Technical Support;
b. if it is established that the Request was not caused by a System Error – close the request at the diagnostics stage by indicating the reasons (source) or providing a consulting service;
c. in the case of every Request related to a Critical Error or a Non-Critical Error, the Contractor's team will implement a Workaround.

Guaranteed response and repair times

Request Priority	Item	Response time (hours)	Time to restore system – use of Workaround (hours)	Repair time (hours)
Priority 1	Critical Error	2	12	48
Priority 2	Non-Critical Error	4	12	72
Priority 3	Fault	6	-	96

If the Error is Software related and the Contractor obtained a diagnosis from the manufacturer indicating that the repair will require installation of a new software version, then the Contractor will provide the Awarding Entity with the content of such diagnosis and implement a Workaround. Once the Awarding entity receives the manufacturer's diagnosis , the Repair Time will be suspended until the Contractor installs new software versions specified by the Software manufacturer.

Planned Works

The Contractor will perform Planned Works in the System provided that the Awarding Entity has been notified and gave its permission within at least 5 days before commencing the works. The Planned Works may be carried out only outside Working Hours.

The scope of the Planned Works will specifically include the following:

1. System Updates;
2. System maintenance;
3. other servicing tasks related to the System and requiring suspending its operation.

9. Instructional Service

The Contractor will provide basic and advanced training in System operation for the users and administrators of the Awarding Entity. The Service will be provided at the registered office of the Awarding Entity. The Contractor will deliver instructional materials in hard copy and electronic format by the day of the given instructional session.
The Contractor will conduct each instructional session on two dates which will be arranged with the Awarding Entity on an ongoing basis. Ten people indicated by the Awarding Entity will participate in every session. Every session will last at least 8 working hours.
After each session every participant will receive a confirmation certificate from the Contractor.

In addition to lecture, every session will include practical exercises conducted in a lab environment made available by the Contractor, identical to the System. The practical part will be conducted on workstations provided by the Awarding Entity, based on the Contractor's guidelines given in the technical concept.

As a result of the instructional service the Awarding Entity's users and administrators must gain all necessary information enabling them to freely operate and manage the System.

The scope of the Instructional Service is as follows:

1) Basic training on System use and operation including at least:
    a. Overview of System architecture;
    b. Reconfiguration related to SSL traffic control – decryption exceptions based on specific traffic parameters (category, Src IP);
    c. Dashboard configuration;
    d. AV filter configuration - file types, etc.;
    e. Local user authentication management – administrator account creation, privilege management, customer accounts, assigning clients to policies;
    f. Reconfiguration of filtering policies;
    g. Adding and editing white/black lists for individual schools;

h. Adding user accounts for individual schools;
i. Configuring school-level reports using automated generation mechanisms based on a timetable;
j. School-level filtering exceptions, based on school IP addresses;

2) Advanced training session in system error processing including at least:
   a. Detailed description of System services, including the purposes of the individual services (for example, Tomcat -> GUI access);
   b. Log analysis;
   c. Service status verification;
   d. Making backup copies of configuration and other data;
   e. Handling System operation errors, specifically related to:
      - policies (why a page was blocked);
      - background services (diagnosis, basic troubleshooting for all elements, including external dynamic content analysis systems);
   f. Handling SSL certificates used in encrypted traffic interception:
      - Certificate validity control;
      - CSR generation;
      - Uploading new certificates;
      - Chaining;
      - Deleting old certificates.

10. Uninstallation of the System after the termination of the Agreement

After the expiry of the Agreement, the Contractor will be obliged to carry out the data erasure procedure at the date agreed with the Awarding Entity. The procedure will be defined in the technical concept and approved by the Awarding Entity. The Contractor and the Awarding Entity will confirm the correct and effective data erasure by signing a certificate confirming the erasure of the data from the Hardware storage media.

After the above certificate is signed, the Contractor will disconnect the System from the Awarding Entity's telecommunications and computer infrastructure, at the Contractor's expense and on the date agreed with the Awarding Entity. The Contractor is liable for all damage caused by its employees during the Hardware uninstallation process and will restore the original condition of the Awarding Entity's telecommunications/computer infrastructure as before the System installation.

The Contractor will collect the Hardware from the data processing centre after both parties will sign a hardware handover report.

V. System Acceptance Criteria

The System Acceptance procedure will involve the verification of the functionality of the system or the performance of the following tasks by the Contractor.

Test	Result (YES / NO)
The System was properly installed and commissioned in the Awarding Entity's telecommunications/computer infrastructure, and can handle traffic from IP addresses specified by the Awarding Entity.	
The System blocks webpages in accordance with the configured filtering policy.	
The System applies different user-dependent filtering policies, based on an external repository (LDAP) and the source IP address.	
The System intercepts SSL traffic in accordance with the implemented policy.	
The System provides a management console for administrators at least through a web interface.	
The System allows for comprehensive editing of filtering policies.	
The System enables traffic report creation/generation/editing based on specific source IP addresses, divided into user groups.	
The System displays an “access blocked” page in accordance with the requirements specified by the Awarding Entity.	
The System allows for customising of the blocked-access page text and appearance.	
The Contractor conducted instructional sessions as specified by the Awarding Entity.	

The Awarding Entity accepted the technical concept submitted by the Contractor.	
The Awarding Entity accepted the System post-implementation documentation submitted by the Contractor.	
The System is compliant with the requirements specified in DCS. (no technical scenarios are required from the Contractor in that regard)	
The Hardware list was verified.	

VI. The division of responsibilities of the parties during the implementation of the project

When preparing its tender and during the implementation of the System and the performance of Services, the Contractor will incorporate the following division of responsibilities:

		Awarding Entity	Contractor
1. Preparation		X	X
1.1	Appointing the Project Managers	X	X

1.2	Delivering a questionnaire concerning the requirements and data necessary for the Contractor to develop the technical concept		X
1.3	Delivering the requirements and data necessary to Develop the technical concept	X	
1.4	Developing the technical concept		X
1.5	Preparing Facilities for installation (for example, providing an uninterrupted power supply and safeguards, ground connection points, etc.) as agreed between the parties	X	
1.6	Ensuring that ambient conditions are compliant with applicable requirements	X	
1.7	Obtaining evaluations and approvals for the technical concept	X	
2. System Implementation			
2.1	Delivering the list of representatives authorised to access the Facility where the System will be installed (min. 5 days prior to the delivery)		X
2.2	Enabling access for the authorised representatives (point 2.1 above), including necessary documents (e.g. permits, individual pass cards, etc.)	X	
2.3	Delivering the System and installation materials in accordance with the technical concept		X
2.4	Unloading the Hardware and the installation materials		X
2.5	Preparing a hardware acceptance report at the data processing centre	X	
2.6	Signing the hardware acceptance report at the data processing centre	X	X
2.7	Connecting the System to the infrastructure in accordance with the technical concept	X	X
2.8	Connecting power supply and ground cables to the Hardware		X
2.9	Software installation, basic configuration and launch		X

2.10	Drawing up post-implementation documentation		X
3. Conducting instructional sessions			X
4. System Acceptance		X	X
5. Support and Technical Assistance Services during the effective term of the Agreement			X
5.1	Delivering a list of representatives authorised to remote access		X
5.2	Enabling remote access for the authorised representatives (point 2.1 above), including necessary documents (e.g. permits, individual pass cards, etc.)	X	
6. System Relocation		X	X
6.1	Preparing Facilities for the installation (for example, providing an uninterrupted power supply and safeguards, ground connection points, etc.) as agreed between the parties	X	
6.2	Ensuring that ambient conditions are compliant with applicable requirements	X	
6.3	Delivering a list of representatives authorised to access both data processing centres of the Awarding Entity where the System will be stored or installed (min. 5 days before the delivery)		X
6.4	Enabling access to the authorised representatives (point 2.1 above), including necessary documents (e.g. permits, individual pass cards, etc.)	X	
6.5	Disconnecting the System from the telecommunications infrastructure of the Awarding Entity		X
6.6	Transporting the System to the indicated data processing centre		X
6.7	Unloading the Hardware and the installation materials		X
6.8	Connecting the System to the telecommunications infrastructure of the Awarding Entity		X

6.9	Conducting System Acceptance after relocation	X	X
7. Uninstallation and collection of the system after the expiry of the Agreement			X
7.1	Conducting effective erasure of the data from Hardware disks		X
7.2	Signing a certificate confirming the erasure of data from Hardware disks	X	X
7.3	Disconnecting the System from the telecommunications infrastructure of the Awarding Entity		X
7.4	Preparing a certificate of hardware collection from the data processing centre	X	
7.5	Signing the certificate of hardware collection from the data processing centre	X	X
7.6	Collecting the System from the data processing centre		X