1. Technical support requirements

1.1 The proposed data leakage protection software product must have a manufacturer-certified technical support center that will provide technical support to users in accordance with the following requirements

- **24x7x365 support –** 24 hours a day, 7 days a week, 365 days a year, including holidays, weekends and non-working days
- **Extended technical consultation** on the configuration and operation of data leak protection software, provided via telephone (with local call feature only, without the use of international calling services) and email.

2. Requirements for resolving data leak protection

2.1 General requirements

- Support to MS SQL Server 2016 and newer versions;
- Support to Azure SQL database server;
- Support to Windows 10 and newer versions, macOS 12 and newer versions;

• Support for Windows Server 2016 and newer versions.
• Integration with MS Active Directory.
• Integration with Microsoft 365, with the feature of monitoring of email and file sharing within the cloud environment, even through unsecured devices.
• OCR technology with multilingual support for content validation.
• Customizable management dashboard based on administrator needs.
• Possibility to define access rights to reports and settings, managed by administrators.
• Stealth mode with hidden processes and folders, even from local or domain administrators.
• System abuse protection mechanisms:

- Protection must be active for all users, including local and domain administrators;
- In case privileged users attempt to terminate processes, the system must revive them or apply alternative methods;
- It must be impossible to delete system components from the device without explicit authorization;
- Editing of the registry, system components, and DLL libraries must be prohibited;
- Unauthorized modification of security settings is not allowed;

- Ensuring protection in safe mode;
- Functionality must be maintained in offline mode without being connected to the company's network.
- Work with archived records;
- Sending reports to SIEM system;
- API integration with Power BI and Tableau for analysis;
- Ability to create backup copies of components and settings.
- Availability of a database manager- storage, area view, creating tasks for storage;
- Scheduled creation of archives and the ability to view them via the management server;
- Automatic notices about incidents via e-mail with sensitivity adjustment and detail refinement capabilities
- Audit of administrator’s actions in monitoring panel;
- Preventive protection through detection of abnormal activity;
- Detection of encrypted archives;
- Automatic achiving of records;
- • Temporary removal of data transfer restrictions with centralized management.
  • Exchange of information search filters.
  • Automatic sending of reports by email with fully customizable format (information volume, monitored users, sending frequency, recipients).
  • Availability of a web dashboard for monitoring security incidents and employee activities.
  • Print control for local, network, and virtual printers.
  • Ability to download the file that caused the data leakage incident.
  • Upon policy violation, not only logging but also incident creation with the possibility to add comments.
  • Policy configuration with dynamic actions that respond to user behavior.
- Configuring web and application access for a user by category.
- Agent installation.

2.2 Information audit
General requirements

- Detailed accounting of application launch and active usage time, by categories.
- Information about the time spent on web pages, including URL, protocol, headers, regardless of browser.
- Export of reports CSV, PDF:
  IM software, web post customers
- Monitoring of data sent, regardless of software;
- Automatic weekly and monthly time usage reports
  E-mail:
- POP3, IMAP, MAPI/Exchange, including SSL:
- Outlook, Thunderbird, Icewarp and other customers, regardless of type;
- Exchange Online –monitoring of user activity, regardless of device.

Data Flow:

• Detailed history of operations performed on sensitive files.

• Local file operations: copy, move, download, delete, device type, source and destination path.

• Search for forgotten confidential files stored on user devices.

• Print data logging.

• Folder content copying, screenshots.

Endpoint activity:

• Power on/off.

• Login/logout.

• Sleep/wake transitions.

Network activity:

• Volume of data downloaded/transferred.

2.3 Data protection
General requirements

- Automatic creation of incidents upon policy violations;

- Software independence, including encrypted connections;

  • Resistance to file protection bypass methods;

  • Classification of sensitive data by application, URL, disk path or content;

  • Use of third-party classifiers;

  • Detection of sensitive files by content, origin, file type;

  • Audit of access to local and network folders, disks and cloud storage;

  • Ability to create shadow copies of files.

Data encryption

- Encryption of the entire disk, including system;
- Encryption of USB drives

Data outflow prevention

- Restriction of sensitive data movement by carrier, website, email address, application.
- Block, notify, monitor modes.
- Blocking user access to Internet resources by URL, domain or category.
- Control of file actions.
- Blocking leaks with specific file extensions.
- Analysis of user behavior with identification of risky behavior.

Monitoring of devices

- General restrictions USB, Firewire, card readers, LPT, COM, Bluetooth, CD/DVD/Blu-ray;
- Monitoring of external devices by creating allowed/forbidden groups;
- With the feature of read-only mode.

Participant Requirements

3.1 A power of attorney issued by the manufacturer, confirming the partnership between the participant and the manufacturer or its official representative and authorizing the participant to submit a price, conduct negotiations and conclude a contract.

3.2 The winning participant must carry out a complete implementation of the System and basic configuration on the buyer's platform.