GREENmod

System supporting the classification of documents and e-mails

TUKAN IT

www.tukanit.pl

Tukan GREENmod

System supporting the classification of documents and e-mails

The problem of confidential information leakage concerns every organization. Whether on purpose or by accident, losing important data happens virtually every day, and is difficult to monitor and stop without special tools. Intellectual property, financial data and personal data of employees and customers may be leaked with the use of many information flow channels, with **losses reaching millions of dollars.**

DLP (Data Loss Prevention) systems, using advanced mechanisms of automatic content classification, omit specific types of content which escape their classification algorithms.

Tukan GREENmod makes it possible to supplement the mechanisms of automatic classification of documents and e-mails with invaluable knowledge of the user regarding the level of confidentiality of the content created by them. This solution integrates with Microsoft Office applications, enforcing the classification of each created document before saving it on the computer's disk. Similarly, Tukan GREENmod prevents sending an e-mail which has not been classified.

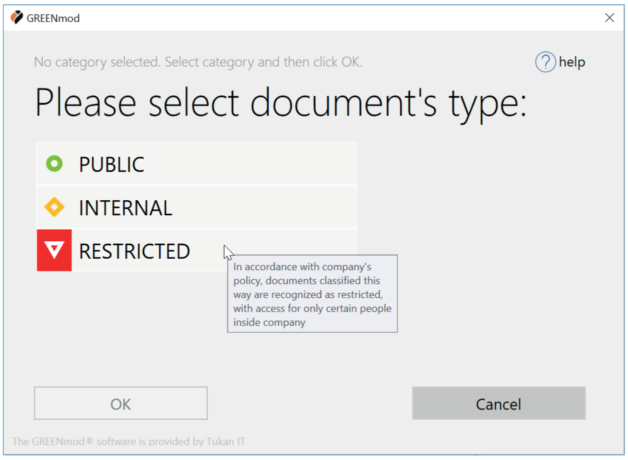
Why Tukan GREENmod?

- Raising security awareness

  Using Tukan GREENmod solution raises employee awareness of security issues and the importance of information processed by them.

- Shifting responsibility for data protection onto document authors

  Organizations' security departments often lack competence to replace business departments and indicate methods of classifying information which may be implemented in DLP systems. The author of the document is the best



No category selected. Select category and then click OK.

Please select document's type:

In accordance with company's policy, documents classified this way are recognized as restricted, with access for only certain people inside company

The GREENmod® software is provided by Tukan IT

The dialog box that appears when you click *Send* in Microsoft Outlook.

source of information about the classification of the outcome of their work. The classification assigned by the user will serve as the first line of protection, supplementing automatic methods of classification provided by DLP solutions.

- ### Easy integration with DLP systems

  The system of marking documents (metadata added to files and e-mails) may be used for automating protection processes such as:

  - monitoring,
  - data transfer blocking,
  - printing prevention,
  - notifying about security breaches,
  - quarantine,
  - data encryption,
  - archiving,
  - search.

Main features:

- ### Forcing document authors to classify documents

  Before saving any new document, Tukan GREENmod will display a dialog box in which the user must specify the document's confidentiality level. This ensures that files which fall outside the description of DLP systems' automatic policies will be properly secured.

- ### Classifying e-mails before sending

  Every e-mail must be classified before sending, which prevents accidental sending of sensitive data outside the organization.

- ### Classifying documents created earlier

  Tukan GREENmod not only enforces the specification of the confidentiality level of new documents, but also makes it possible to classify the ones created before its installation. Upon opening an unclassified document, the system may ask the user to specify the desired protection level.

- ### Easy identification of the document's author

  The system may add the name of the logged-in user to files' metadata.

- ### Ensuring compliance

  By enforcing the classification of each new document, Tukan GREENmod ensures compliance with internal and external regulations, such as Recommendation 'D' of the Polish Financial Supervision Authority, addressed to financial institutions or Regulation of the Prime Minister regarding methods of security classification. The type of classification and marking can be freely modified.

- ### Possibility of customizing the classification structure

  The solution provides full flexibility of defining classification levels, together with their embedding, which ensures better definition of the protection level and the type of created document. For example, confidential documents may be divided into supplier agreements, customer agreements or drafts of new services, and may be secured by DLP systems in various ways depending on the needs.

- ### Flexible configuration of the content of application elements

  The solution supports multiple languages and makes it possible to define all elements of the screen interface displayed to end users (e.g. dialog boxes, help bubbles or colors of buttons and icons).

- ### Protection against lowering the classification level

  Tukan GREENmod protects against lowering the classification level, thus preventing an accidental or purposeful leakage of sensitive information. For example, it is not possible to mark an e-mail as public (open) if it contains an attachment with higher classification.

- ### Integration with DLP systems – reducing the risk of information leakage

  The document marking method used in the solution may be used for securing documents by DLP solutions protecting against data leakage. The classification information, included in the file's or email's properties, enables a DLP system to apply a relevant security policy adequate for the protected content.

- ### Integration with Data Exchange Layer

  The solution ensures integration with McAfee Threat Intelligence Exchange/Data eXchange Layer (TIE/DXL), enabling sharing information (about access to classification) between other IT security solutions such as SIEM systems (e.g. McAfee Enterprise Security Manager), DLP systems (e.g. McAfee DLP) and between other products.

- ### Central management and reporting

  Tukan GREENmod provides an intuitive management dashboard which enables remote software distribution, configuration management and collecting events related to content classification. In addition, the system makes it possible to monitor the activities of users which are related to document classification and access to protected information.

- ### Flexible distribution methods

  The software may be distributed to end stations through a dedicated management console or popular installation methods used by enterprises, such as Microsoft SCCM, Microsoft Active Directory Group Policies or McAfee ePolicy Orchestrator.

- ### Support for various versions of Microsoft Office

  The solution is compatible with Microsoft Office 2003, 2007, 2010, 2013 and 2016. Subsequent versions will be extended to support other systems.