DATA LOSS PREVENTION SOLUTION

Is there any DLP solution affecting the application: Yes  No

If yes, indicate which of the controls have been activated for the application:

|  |  |
| --- | --- |
| **Control** | **Activated?** |
| Identification of personal / sensitive data | Yes    No |
| Classification of personal / sensitive data | Yes    No |
| Monitoring of activities involving personal / sensitive data | Yes    No |

Indicate the types of monitoring covered by the DLP solution:

|  |  |
| --- | --- |
| **Monitoring type** | **Controls enabled** |
| Data at rest | Restrict access to local administrative functions, such as the ability to install software and modify security settings. Prevent malware, viruses, spyware, etc.  Prevent copying of confidential data on unapproved media. Verify that authorized data extraction occurs only on encrypted media. |
| Data in use | Monitor access and use of high-risk data to identify potentially inappropriate use.  Restrict user skills to copy sensitive data into unapproved containers (for example, email, web browsers), including control over the ability to copy, paste and print sections of documents. |
| Data in motion | Prevent unencrypted sensitive data from leaving the perimeter.  Record and monitor network traffic to identify and investigate inappropriate transfers of sensitive data. |
| Active monitoring of Data Leaks | Verify that remote access to the corporate network is protected and control data that can be saved through remote installations, such as Outlook Web Access. |
|  |  |
|  |  |
|  |  |
|  |  |