**<Provider Company Name>**

<Addressee Title>

<Addressee Name>

Registration no. \_\_\_\_\_\_\_\_\_ «\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_.

**Rules of Engagement**

By this letter <Customer Company Name> (hereinafter – the Customer) represented by <responsible manager’s title and full name>, acting based on <Statute, PoA etc.>, authorizes <Provider Company Name> (hereinafter – the Provider) represented by the specialists of the project team acting according to the Service Agreement No. <agreement number> “\_\_\_”\_\_\_\_\_\_\_\_\_\_20\_\_\_ (hereinafter – the Agreement), to perform the assessment of the Cutomer’s information infrastructure security against external (internal etc.) attack.

The Customer confirms that the following ranges of IP addresses belong to them:

The Customer undertakes the responsibility to notice their Internet Service Providers about the planned penetration testing activities including the time frame of the testing.

The Customer recognizes that all Provider’s actions related to fulfilling the contract obligations according to the Agreement are not malicious and are not aimed at the compromise of confidentiality, integrity or availability of information that circulates, is transmitted or processed in the Customer’s network.

The Customer recognizes that all actions of the Provider related to fulfilling the contract obligations according to the Agreement are aimed at the improvement of performance of the Customer’s network through searching its vulnerabilities and their functional validation by using them inline with the terms of the Agreement.

In particular, in order to verify the validity of discovered vulnerabilities of information systems and risk assessment of potential exploitation of these vulnerabilities the Provider receives the Customer’s authorization for performing the following actions:

1. Using discovered vulnerabilities to gain access to the Customer’s information systems;
2. In case of successfully receiving access to the Customer’s information systems:
   1. Continuation of assessment of this information system as well as systems and networks connected to and interacting with this system;
   2. Attempting to gain access to related information systems;
   3. Attempting to escalate the privileges of obtained access;
   4. Attempting to gain access to business critical data an information in order to demonstrate actual information security risks.
3. Testing information systems’ password security by performing password guessing;
4. Testing cryptographic security of hash and otherwise protected passwords.

The authorization extends to all Customer’s information systems within the security assessment project scope. The authorization is valid on weekdays from 09-00 to 18-00 within the time period between “\_\_\_” \_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ and “\_\_\_” \_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_.

Actions of validation and using discovered vulnerabilities are performed by the Provider after informing the authorized single point of contact at the Customer’s side and obtaining the corresponding permission by email.

Provider’s project team:

Customer’s authorized single point of contact:

**The Customer**

**<Title>**

**<Customer Company Name>**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ <Signee Name>**

**<Stamp>**