1. Backup the files up.  
   PECZARB advised E3T to have a backup solution of uploading database (and root files of the web-application) to another server. In this case, if the production server behaves unexpectedly, the company will have a chance of restoring all the lost (or corrupted) data.  
   E3T has approved this decision.
2. Having a fallback router.  
   The team has proposed that the network infrastructure should have two routers. If the main one fails, the whole system will not stop functioning, but the connections will be redirected through the second “backup” router.  
   Team’s network design was approved by the client.
3. Using multiple servers.  
   Network design shows 3 servers – for database, for web-application, and for Active Directory. This is a common practice to make use of multiple servers as it will be almost impossible to get the whole system down.  
   As was mentioned, E3T approved the proposed network drawing.
4. Rejection of non-SSL requests to the web-application.  
   Every unsecured HTTP request is being responded with the proposal to use HTTPS. Thus, every piece of data transmitted to and from the user is encrypted and will be readable only among the user and the server. According to CIO (US’ Federal **C**hief **I**nformation **O**ffice), [it is a common practice to make use of HTTPS for everything](https://https.cio.gov/everything/).  
   The client agreed to the point made by CIO.