|  |
| --- |
| DEPARTMENT OF SOCIAL PROTECTION |
| Structure and Use of SharePoint |
| In the Department of Social Protection |
|  |
| **Rachel Byrne X00109827** |
| **20/04/2016** |

|  |
| --- |
| This report will discuss the basic overview of SharePoint and how the Department of Social Protection enforces this service. |

## Basic introduction to SharePoint

SharePoint is a web application platform in a Microsoft Office Server suit. It combines various functions which are traditionally separated applications such as Intranet, Document Management, Workflow Management and Web Content Management.

SharePoint can be used as a secure place to store, organise, share and access information from almost any device. SharePoint servers have traditionally been deployed for internal use in mid-size businesses and large departments.

Installing SharePoint on the departments premises required multiple virtual machines with two separate servers and is a somewhat significant installation and configuration effort.

## Use of SharePoint in the Department

'Stór2' is the Department of Social Protections current form of SharePoint. SharePoint is used vastly in the department as the departments intranet. It is used to collaborate team work, provides clock-in and clock-out functionality and payment displays (payslip). 'Stór' is used to provide information about every employee in the department that everyone can see and private information such as payroll numbers. It is a form of communication, work flow management and a recording system for both projects and daily login activities.

For each project that is taken part in the Department be it by BOMi Design& Development Team or Service Delivery Model Team, each project gets an individual team site for that project which only team members involved in the project and the customers are allowed to access.The team sites provide an area to share and display documentation related to the documentation. There are other functionalities available on the team sites including work items.Work Items displays all the tasks that have been set up for the project it provides information such as what team member is the task assigned too, whether it is done or still pending and all the information about what needs to be done.

SharePoint allows the design team to connect with Visual Studio and create a Team Foundation Server (TFS). This functionality helps you to learn to work with your code, used mainly by customers. It also provides a record of all the builds done in the TFS which can help if there is any bugs, which can provide a rollback state to a point where the system worked properly if and only if, the bug has been deemed too difficult to fix.

SharePoint also provides Team Rooms to allow team members to communicate and share screens. SharePoint creates Project Management Schedules and will show you the timeline of the project iteration you are currently on and the next iteration on the way.

An employee cannot create a 'Stór' account themselves, they are only created when an Assistant Principal requests an administrator to create an account for the incoming employee.

## Advantages and Risks Involved in Blocking/Un-Authorizing access to files

Blocked files in SharePoint should be evaluated and considered when planning out Goverance or security of SharePoint deployments.

There an both advantages and disadvantages of blocking access too files for employees.

### Advantages

There are multiple security advantages of blocking access too files from unauthorized users. Unauthorized users in the case of the department are employees that are not a part of the team site they are trying to access.

By blocking access to files it ensures that no information about projects taken part within the department could fall into the wrong hands, as outside customers are given access to the project team sites but if they were able to access all information and documentation shared on 'Stór' they could leak Government data or allow outside access into 'Stór'.

It also allows administrators to control a large number of Blocked File Types, to ensure no data is corrupted.

### Blocked File Types

Blocked File Types are a security feature in SharePoint that allows SharePoint or 'Stór' administrators to specify certain files from being shared or accessed in the SharePoint environment.

These are used rarely in the department but administrators block employees from viewing files and only granting access to employees that are regulated and confirmed by their Assistant Principal that they are a part of a certain team and should be allowed to access the team site created for the project they are on and all documentation shared within this team site.

### How does it work

In the case of Blocked File Types, SharePoint will check a file name and any characters immediately after a period (.). If a set of characters after a period is matched against a set of characters in that blocked file list, it will block that file.

In the department, SharePoint will check the current login user against the database to see if they have been granted access too files. When an employee logins to their desktop they are automatically signed into their 'Stór' account. On their profile it will display all team sites they have access too. If the employee clicks on a team site, a link or a file that they do not have access too a warning will appear and will allow them to request access with a comment explaining why they need access, they will then contact the users Assistant Principal to confirm their request.

### Disadvantages

Even though there are many advantages to blocking files there can be disadvantages also. There is a lot of database configuration and overhead and can be very time consuming for administrators. It can also delay time for projects as some team members may have not been giving access to sites and programs that they may need to use for their project.

## How Do I Block/Unblock files?

Administrators are the only people within the department that can block and unblock files.

### Block File Types

To unblock a file type these are the steps the administrator takes:

1. Login to the Central Administrator site.
2. Central Administrator > operations > security configuration.

To unblock files , it involves simply removing the .dot extension from the list.

To add files to be blocked the administrator adds its extension to the list. If you want to unblock a file type then just remove the extension for that file type from the list. There can be limited too 1024 different types of files.

### Users

To block and unblock users the steps an administrator must take are:

1. Login to the Central Administrator site.
2. Central Administrator > operations > security configuration.

To add users the administrator will add the employee to the file using a database extension and for unblocking simply removing the employee from the file extension.

* A person is granted access to a file when they request access and this access is confirmed by the employees Assistant Principal(AP).

## Protecting Data

When coming up with Data Protection laws, a data protection team sat together with database administrators and developers and created the data procedures by adopting a view of data protection from the application perspectives.

The adoption to SharePoint servers have led to existing file servers being replaced by SharePoint servers. These servers allow employees to access documentation via SharePoint web portals and Microsoft SQL Servers. SharePoint largely consists of SQL Server databases that have efficiently planned data protection strategy for Content recovery and Disaster recovery. Another approach is to simply back up or protect those databases using the tried-and-true approach.

Two recycle bins at a user level and site level are used to stop files from being deleted permanently which will help speed up recovery.

This can be done by a data protection team or through a third party , an example DocAve 4.1 suite that has the ability to perform live backups without suspending indexing.

Most department content resides in SQL Server or Shared Service Provider(SSP) databases and most configuration data resides in the configuration database. However SharePoint does also depend on front-end server components such as binary files, registry hive and customisation.

### SharePoint data protection layers

SharePoint has three logical tiers of data protection layers , these are based on how often data is typically recovered at each one.

1st: Logical layer one provides data recovery for data loss that is often user driven such as accidental deletions or corruption of files. Site administrators or end users perform the tasks to restore the data.

2nd:The second logic layer provides more advanced backup and restore tasks done by administrators at the farm level, including data restoration and business continuity in case of hardware failure, migrations or database operations.

3rd:The third layer provides back up for disaster recovery this entails designing the infrastructure in such a way to ensure high availability by redundancies and eliminating single points of failure.

## Attacks

Due to data protection I cannot discuss any attacks that have been made to the departments 'Stór'. In the result of the attack the decision to not allow any user create their own account but only be created by an administrator.