**High Level Design: New Learning Solutions**

Cable Davis

Department of Education, Concordia University

ETEC 651: Fundamentals of Human Performance Technology

Dr. Ann-Louise Davidson

March 10, 2020

**Part A: Roadmap**

**Overview of the Interventions**

* Write an Information Security Policy
	+ Format: Official Policy
	+ Communication Medium: Company Website
	+ All Objectives (See Appendix for objectives)
	+ All Performers (See Appendix for phases of performance)
* Create an IT Specialist Role
	+ Format: Job Description
	+ Communication Medium: Memo/Online job board
	+ All Objectives
	+ All Performers
* Invest in a Secure File Management System
	+ Format: File Explorer
	+ Communication Medium: How-to Video
	+ All Objectives
	+ All Performers
* Establish Hardware Security Standards
	+ Format: Checklist
	+ Communication Medium: Electronic Fillable Document
	+ 1st Objective
	+ All Performers
* Establish a Software Security Standards
	+ Format: Checklist
	+ Communication Medium: Electronic Fillable Document
	+ 1st Objective
	+ All Performers
* Develop a File Confidentially Job Aid
	+ Format: Job Aid
	+ Communication Medium: Electronic Document with Hyperlinks
	+ 3rd Objective
	+ Unsure and Confident Performers
* Develop an Information Security Training
	+ Format: Live Training
	+ Communication Medium: Online
	+ 2nd Objective
	+ Unsure and Incognizant Performers
* Provide Quarterly Information Security Feedback
	+ Format: Checklists
	+ Communication Medium: Email
	+ All Objectives
	+ All Performers

**How the Interventions Interrelate**

**Part B: Intervention Descriptions**

**Write an Information Security Policy**

 Create a committee to write a new information security policy for New Learning Solutions. This committee will be filled with a variety of experts such as, the founder, a trusted client representative, an information security expert, and an employee who is a ‘confident’ performer. The committee members can create a document that will have an overarching plan for how the company is to handle information security by using their collective expertise.

|  |  |
| --- | --- |
| Performance Needs Addressed? | This addresses the lack of information and resources to employees. |
| Level and Phase of Performance Addressed? | This addresses performance at an organizational level and all performers. |
| Performance Objectives Achieved? | This helps achieve all performance objectives. |
| Format & Expectations? | This will take the form of a company policy. A policy is expected be formal and deliberate |
| Communication Medium? | This should be posted on the company’s website. This creates transparency and allows all performers to view it. A possible limitation is that it is tied to the web, so if the website goes down so does the policy. |
| Bottom Line: Why this Intervention? | A new policy that is widely available sets a clear goal and standard for management, employees, and assures clients that NLS will treat their information with care. |

**Create an IT specialist role**

The founder, along with an information security expert, should create a job description and estimated salary for an IT specialist for the company. Part of the duties of the IT specialist would be to manage information security for the company using some of the other interventions provided as well as other specified tasks. This role should first be offered internally to ‘confident’ performers and then externally if no one wants to fill this new role.

|  |  |
| --- | --- |
| Performance Needs Addressed? | When the role is filled, this addresses a lack of resources available to the employees. |
| Level and Phase of Performance Addressed? | This addresses performance at an organizational level and all performers. |
| Performance Objectives Achieved? | This helps achieve all performance objectives. |
| Format & Expectations? | The role should be described in a manner that matches other job descriptions. This includes expectations for the job, experience required, and pay. |
| Communication Medium? | When offering this job internally, this should be first released as a PDF memo. If offered externally, this should be posted on an online job board. Using both communication mediums mitigates most foreseeable limitations. |
| Bottom Line: Why this Intervention? | NLS has no official IT role within the company. The founder and some employees often take this mantle when needed, but as the company grows this role needs to be cemented and provides a clear point of contact for employees. |

**Invest in a Secure File Management System**

 Whether going with a third-party provider or deciding to do it locally, it is necessary that the central storage of files and information for the company is secure. This file management system should be used for not only storing but also sharing files between employees of the company. The IT specialist can manage this system as one of their duties.

|  |  |
| --- | --- |
| Performance Needs Addressed? | This addresses resources available to the employees. |
| Level and Phase of Performance Addressed? | This addresses performance at the organizational level. This affects performers at all levels. |
| Performance Objectives Achieved? | This helps achieve the third objective. |
| Format & Expectations? | A file management system can be integrated into a user’s existing file explorer (Finder on Apple). The user expects that the folders will be labeled accurately and consistently. |
| Communication Medium? | A brief how-to video should be produced or found on YouTube that gives instructions on how to use the file management system. This is a system that is often difficult to explain with words, so visualization will help performers understand this system. Those with experience in remote work will find this concept simple, but the less experienced may need additional help. |
| Bottom Line: Why this Intervention? | This prevents sensitive files from being leaked because they were stored on an employee's personal storage or shared via an insecure medium. |

**Establish Hardware Security Standards**

 Using the newly written information security policy, the IT specialist and an information security expert will elaborate the hardware standards of employees’ devices. These standards can then be used to ensure all current and future employees are using acceptable hardware for doing work.

|  |  |
| --- | --- |
| Performance Needs Addressed? | This addresses a lack of information by providing clearer standards. |
| Level of Performance Addressed? | This addresses performance at the organizational level. This affects performers at all levels. |
| Performance Objectives Achieved? | This helps achieve the first objective. |
| Format & Expectations? | This will take the form of a checklist. Performers would expect a list of statements that clearly define expectations of their hardware. |
| Communication Medium? | This checklist should be created as a fillable electronic form. This allows the key data to be exportable into a spreadsheet for the IT specialist. A disadvantage is that this may not cover all the unexpected aspects of the hardware or all kinds of hardware. |
| Bottom Line: Why this Intervention? | One of the basic tenets of information security is that the hardware that a user has is secure. This can be done by ensuring that a device has a password lock, does not AutoRun external memory devices, and does not appear to be broken into, etc. |

**Establish Software Security Standards**

 Created in a similar fashion to the hardware security standards, the IT specialist and information security expert should specify software standards required of employees’ devices. These serve as two different interventions to ensure that each set of standards receives the attention needed for each to be effective in their implementation.

|  |  |
| --- | --- |
| Performance Needs Addressed? | This addresses a lack of information by providing clearer standards. |
| Level of Performance Addressed? | This addresses performance at the organizational level. This affects performers at all levels. |
| Performance Objectives Achieved? | This helps achieve the first objective. |
| Format & Expectations? | This would take the form of a checklist. Performers would expect a list of statements that define expectations of the software installed on a work device. |
| Communication Medium? | This checklist should be created as a fillable electronic form. This allows the key data to be exportable into a spreadsheet for the IT specialist. A disadvantage is that this data could get unruly as there is a plethora of different kinds and versions of software. |
| Bottom Line: Why this Intervention? | Ensuring that employees’ devices are up-to-date and have security software installed prevents hackers and other nefarious Internet users from getting sensitive company information. |

**Create a File Confidentiality Job Aid**

 Employees need to be sure what files are sensitive and which are more public, and a job aid can provide clarity on this. This job aid can be created with input from an information security expert and the new IT specialist for the company. The job aid should create a hierarchical list of confidentiality, examples of files at each of the levels, and how to properly label files of each type.

|  |  |
| --- | --- |
| Performance Needs Addressed? | This address a lack of information and resources available to the employees |
| Level of Performance Addressed? | This addresses performance at an individual level and addresses ‘unsure’ and ‘confident’ performers. |
| Performance Objectives Achieved? | This achieves the third performance objective. |
| Format & Expectations? | This would take the form of a job aid. This should be written so it is easy for the performer to find relevant information and provide clearly labeled how-to instructions. |
| Communication Medium? | This can be done by using an electronic document with hyperlinks that quickly leads to the relevant sections needed by the user. A limitation of this format is that it would be difficult to apply to physical documents. |
| Bottom Line: Why this Intervention? | This intervention is needed to prevent internal information leaks. It also serves as a constant reference point for employees without having to reach out to the IT specialist. |

**Develop an Information Security Training**

Over the course of a day, an instructor will deliver a series of training sessions that review the best practices and basic tenets of information security. The trainings will include information about how to keep information private online, how to prevent fraud, and what kinds of software can enhance online security.

|  |  |
| --- | --- |
| Performance Needs Addressed? | This addresses a lack of skills and knowledge in employees. |
| Level and Phase of Performance Addressed? | This addresses performance at an individual level and performers at the ‘unsure’ and ‘incognizant’ levels. |
| Performance Objectives Achieved? | The second performance objective. |
| Format & Expectations? | This will be a live training. Performers expect an informed instructor, handouts, and responsive feedback. |
| Communication Medium? | This training can be done online. This is advantageous because it allows the employees to complete the training anywhere. A disadvantage is that the technical set-up required could be arduous.  |
| Bottom Line: Why this Intervention? | A live, online training would be an easy and accessible way to ensure performers are aware of the threats that face information security and how to protect against them. |

**Provide Quarterly Security Feedback**

 One of the duties of the IT specialist will be to provide feedback to employees on a quarterly basis using the hardware and software security checklists. The employee and IT specialist can schedule a time for the employee’s chosen device can undergo diagnostics. The results can then be sent to the employee with feedback for improvement.

|  |  |
| --- | --- |
| Performance Needs Addressed? | This addresses a lack of information in the performers |
| Level of Performance Addressed? | Feedback addresses performance at an individual level and is still able to target all groups of performers. |
| Performance Objectives Achieved? | This helps achieve the first and second performance objective. |
| Format & Expectations? | Feedback should be given by the previously mentioned checklists that clearly state what met and failed the diagnostic. A stated path for improvement is also expected by performers. |
| Communication Medium? | Feedback can be communicated over email. This gives the performers a written document to refer to. A possible disadvantage is that performers need further clarification, which could be better resolved through an in-person meeting. |
| Bottom Line: Why this Intervention? | Feedback creates an open and constant line of communication between the IT specialist and employees. This regular feedback provides employees with the information they need to continue to be successful and perform as expected from this campaign. |

**Appendix**

**Performance Objectives**

1. Informed about security policies, performers ensure that devices are securely configured for work purposes 100% of the time while working
2. Given security policies that define secure web use, performers apply appropriate software to browse the web 100% of the time when using the web for work
3. Given a job aid that identifies level of confidentiality for files, performers apply appropriate confidentiality measures when managing work files 100% of the time

**Phases of Performers**

1. Unsure – Performers aware of information security threats but not aware of how to address their concerns
2. Incognizant – Performers who are unaware of information security threats
3. Confident – Performers who are aware of information security threats and are aware of how to address some of their concerns