2020

IT Security Plan

Supervised by:
Dr Zhe Wang

Submitted by:

Mr. Heang SOK_s5204340; Mr. Jingdi LIN_s5210032

Assignment Group 119

Table of Contents

IT Security Plan

1. Introduction

Planning is the first and foremost important criteria in every management level, includes IT security management. A decent IT security plan ensures that the confidentiality and integrity of data or information is available to the right person, in the right format at the right time. In the absence of planning a manager could become a victim of circumstances (Ufartiene, 2014). According to an empirical research conducted by Alipour, Arabani, Asadi, and Zareii (2013), a sufficient planning could bring forth the following benefits to an organisation:

- Managers are able to produce the beneficial business decision making that aligns with the organisation's goal
- It could reduce overhead cost and time saving: effective working experience
- It offers steady growth and opportunities to the organization for the desired future.

Due to the recent incident of Covid-19 virus, Remarkable University is launching a new online learning platform to cope with the current situations. The university has to ensure that all risks and threats associated with the new platform are identified in term of information security and the protection of the university information resources. The deployment of the new online learning platform should be done properly in a way that secures against common automated and simple manual attacks. Barik and Karforma (2012) pointed out in their research paper that there are risks out there that could compromise the university's IT assets. These risks includes confidentiality attack, integrity violation, availability attack, cros-stie scripting (XSS), denial of service (DOS), masquerade, and malicious program (Barik & Karforma, 2012; Kumar & Dutta, 2011). Kumar and Dutta (2011) stated that in order to create a secure and reliable online learning environment it is important for the university to remove all the security flaws and come up with a decent IT security plan and policy.

The Remarkable University's policy covers all university IT assets and conforms to Queensland Government Information Security Controls Standard (2020). It applies to all stakeholders includes business partners, administrative staff, tutors, and students (alumni and current students). Literally, having the policy is a must for the university because it keeps all stakeholders safe and be preventative (Reimer, Simpson, Hajer, & Loxley, 2009). As for information security policy, all stakeholders would be proactive and protective from cyber-attacks. The Remarkable University information security policy ensures that:

- All strategic and IT assets are designed for education purposes only (research, teaching, and learning).
- Confidentiality, integrity and availability of individuals data are protected.

- All users have responsibilities to conform to these policies when using university IT assets.

2. Key IT Assets

Before conducting a risk assessment, it is crucial to explore and identify all key IT assets first. This is because key IT assets are potential keys that are needed for any organisation to utilise and manipulate its resources effectively. According to Stallings and Brown (2015), IT assets refer to any information technology equipment and systems owned by an organisation.

Table1 illustrates the overview of IT Assets in categories.

Table1: Overview of IT Assets

Categories	IT Assets
Hardware	Desktops, Laptops, Printer, Scanner, switches, hubs, routers, monitors, keyboards, mics, web/application servers, and other peripherals.
Software	• Operation system (Window, masOS, Linux) • Learning management system (LMS)
Data	• Databases
Communication lines and networks	• Mail system • Local area network system (LAN)/network channels and facilities

As shown in table 1, there are many assets associated with this online learning environment; however, only 5 components are considered as Key IT assets for the Remarkable University. The first important key IT asset is web/application servers, for it allows both webpages and applications to run remotely. In other words, a web/application server is a centralised device that store databases for later usage. These stored data could either be generated automatically by application or created by personnel. Therefore, it needs to conform to CIA Triad (confidentiality, integrity, availability). Due to the fact that learning management system (LMS) also associated with CIA Triad, it is listed as a second key IT asset. LMS is an effective and practical software application that is widely used today in the online education sector. It allows the automation of delivering learning material, training programs, tracking marks, and documenting. Hence, it relies heavily on web/application servers. The third key IT asset is databases. It is important for the university to check the integrity of the stored data and make sure that there is no modification. For that reason, the receiver of the data should have all the original state of information that the creators intended them to have. The next key IT asset is the mail system since it is inevitable to use the mail system to encode and decode messages between tutors and students, especially in the online learning environment. Literally, it has to be in the confidentiality and integrity states. Lastly, a good standard Local area network system (LAN) or network channels and facilities could build confidence between tutors and students and advance their cognition relationship. The university has to ensure that communication networks are rendered available to those who need them. Thus, LAN is weighed as one of the key IT assets.

3. Risk Assessment

Having defined and explored the key IT assets, it is time to conduct the risk assessment. Risk assessment is a very critical process in IT risk management because it ensures that all key IT assets will be deployed effectively. Ideally, every IT asset should be examined and evaluated in the risk assessment process. However, it would cost a tremendous amount of money and time. Therefore, in a typical situation, a risk assessment would be used to examine and evaluate only key IT assets. The risk assessment process mainly focuses on analysing the risk likelihood, risk consequences, and risk level.

3.1 Web/Application Servers and Databases

The main issues for web/application servers and databases is authentication and access control and the risk likelihoods for these two assets are considered as “Likely” because servers and databases are a type of IT assets that purposely designed to communicate data with third parties through a target network, thereby it is frequently under the attack of intruders. Professional hackers could simultaneously attack and breakthrough server systems by launching automated botnet attack to gain access to the university’s database and server systems. On the other hand, another concern with databases and servers is integrity as sensitive information that transmitted between the web/application server and the clients (web browser) could be intercepted and modify across the network. Normally, databases could be attacked by either internal (administrative staff, tutors, and students) or external threat in term of dictionary or brute force attacks. If an intruder gain access to the university’s database system, it could lead to potential problems like file modifications or fabrications and revealing sensitive information. In a worse scenario, the intruder might manipulate those sensitive information to extort money from administrative staff, tutors, students, or the university principal. The second risk relates to network security. Sometimes the attackers do not have the intention to steal sensitive information, but they may try to compromise the availability of users to access to the database servers. A common attack like Distribute DOS (DDOS) would flood the bandwidth and compromise data traffic in which slowdown webpage loading. This would result in dissatisfaction of the user groups such as tutors and students. Moreover, it could distribute to ineffective and impractical online learning experiences for students. Third, the web/application server and database assets also associate with the risk of software security because these assets are operated by a type of application such as MYSQL, Oracle, or SQL Server. SQL Injection (SQLI) is a widely known attack on database and server systems. The attackers could attack the university by using SQL Injection to bypass those types of application securities and execute malicious SQL statements that are able to manage the database server behind the university web application. Next, since the server and database systems needed to operate 24/7, it is critical to take physical security into consideration. According to Stallings and Brown (2015), physical security includes environmental threats, technical threats (over or under-voltage), and human-caused threats. Ideally, natural disasters like tornado, earthquake, and bushfire could occur and post damages to the university’s database and server systems. In addition,

over or under-voltage could cause the systems and logic units to shut down or errors. Lastly, the database and server systems also involves with human resources security. Stallings and Brown (2015) shown that employees' behaviours or actions could lead to security compromised, errors, and fraud. This category includes both intentional and unintentional behaviours that could post a great threat to the accountability of the university database and server systems. Therefore, risk consequence for these assets is "Major" and the risk level will be "Extreme".

3.2 Learning Management System

As detailed in section 2, learning management system (LMS) is a type of software application associated with the CRUD user interface that conforms to CIA Triad. For instance, the tutors could update or delete course contents every week, and the students could review the course contents or marks. In term of web and network security, a common threat that targets LMS is cross-site scripting (XSS) attack. Though LMS is usually well-built under the NIST Cybersecurity Framework, it still possibly be attacked by cross-site scripting (XSS) due to mistakes that developers made during coding. Normally, the attackers use automated scanning and exploit tools to scan for the vulnerabilities in LMS as well as other web applications' codes before attacking. The detrimental impact of XSS on LMS usually leads to monetary loss as an attacker could possibly use account hijacking technique to steal credential or sensitive data like credit card numbers. In term of user authentication and access control, Kumar and Dutta (2011) portrayed that, in general, the attackers would attack LMS by using a brute force attack to predict users' passwords and usernames. Another common attack is session hijacking. They pointed out that once the attackers hijack a session, they could gain access to a server without the need to authenticate to the server application as long as the communication session remains active. This is a type of attacks on confidentiality that lead to a sensitive information breach. On the other hand, the vulnerability of LMS's software security usually results from poor programming practices. Ideally, it is crucial for programmers to avoid making any mistakes while coding; however, conducting mistakes is inevitable sometimes. Software coding errors may exist because of incorrect calculation of buffer sizes, deployment of potentially dangerous functions, integer overflow or wraparound, and so on. This issue would influence LMS software quality and reality which leads to users' dissatisfaction. Forth, LMS is mainly operated with database servers, for database security will be discussed in this part. The attackers may try to discover the vulnerability in LMS, and then send malicious code to the university database servers to be executed. The consequence of this attack includes the loss of monetary or sensitive information. Due to the descriptions above, the risk likelihood for LMS is rated as "possible", and the risk consequence is considered as "Major". Therefore, the risk level is "Extreme".

3.3 Network Channel and Facility

Network channel and facility asset mainly focuses on the availability of information because it works closely with the data link and network layers in OSI model. In the

wireless network context, there are several approaches that a hacker could deploy Denial of Service (DOS) attacks and block the network from render available to users. One example of these approaches is TCP/IP 3 Ways Handshake which denies network access to all legitimate requests through the network channel. In contrarily to Phishing and brute force attack, Denial of Service attack (DOS) does not have an attempt to steal data information, its purpose is to ruin an organisation's operation, reputation, and goodwill; this problem would consume a lot of time and money before the organisation could recover. However, nowadays, programmers design operating systems to avoid TCP/IP protocol errors; and because of programming advancements, it is very difficult for a single hacker to take down the network channel and facilities. So, this asset risk likelihood is classified as "Unlikely". Moreover, network channel and facility asset also involves with physical security. As mentioned in database and web/application server assets section, physical threats include natural disaster, such as earthquake, bushfire, etc., could damage the university's network devices such as network wires, routers, switches, and gateways. Though such a disaster would be very rare in Australia, the IT professional should take it into account, and be proactive. Stallings and Brown (2015) advised that network facility such as routers, switches, and gateways may associate with malicious software which compromises the operating system security. In this scenario, the network devices are configured in advance with malicious BIOS software that functions to steal users' passwords or data. Therefore, selecting a trustworthy network device brand is very critical. Lastly, there are threats involves with human resource security. For example, some university staff might make an unauthorized access to network devices. This type of action could distribute to other risks, such as theft, vandalism, and misuse (Stallings & Brown, 2015). It could be concluded that the risk consequence in this asset is "Major", and the risk level is "High".

3.4 Mail System

With the advancement of internet technology, email has become a powerful means of communication due to the cost and time effective manners. It allows different user groups in an online education environment such as tutors and students to correspond regularly anywhere and anytime. Thereby, it has to be confidentiality, integrity, and availability. This is because emails contain privacy information that users, such as administrative staff, tutors, and students absolutely want to be safe from other people. Stallings and Brown (2015) suggested that email has become a powerful weapon used by hackers, for 90% of all emails were reported as spam emails. For this reason, the risk likelihood in the mail system is listed as "Likely". With the reference to network security, Stallings and Brown (2015) pointed out that these spam emails is most likely used for scamming, carrying malware, and Phishing attempt. However, today users have been familiar with spam email and receiving spam emails is safe as long as the users do not click the contents inside those spams. Since the email system requires users such as administrative staff, students, and tutors to have their unique password, it also relates to user authentication and access control. The pro of using password-based authentication is because it is costless and easy to setup. However, there is a few issues with setting up a password. For example, the password maybe generated from common words which makes it easy for the attackers to use dictionary attack or

brute force attack. Users group like students might also write down the password and keep it under the keyboard or stick it to the monitor. These activities could lead to the vulnerability of email authentication. Regard to human resource security, Stallings and Brown (2015) implied that users within the online learning environment might misuse the advancement of email to conduct inappropriate behaviours that has a detrimental impact on the university's reputation, for example, harassment emails. Lastly, malware like Trojans and Ransomware could be sent to students, administrative staff, and tutors by email which posts a great threat to the operation system and files security. Unlike a worm, these types of malwares could run based on Window or MacOS operation system to compromise the operation system security and let other malware in, or it would lock down users' computers and files, then extort the users to pay for the attackers. Hench, the risk consequence is "Moderate", and it leads to the risk level of "High".

3.5 Risk Register

The detailed of risk register has been shown in Table 2 below:

Table2: Risk register

Asset	Threat/Vulnerability	Existing Control	Likelihood	Consequence	Level of Risk	Risk Priority
Web/application servers	• Web/network security • User authentication and access control • Software security • Physical security • Human resource security	Not applicable	Likely	Major	Extreme	1
Databases	• Web/network security • User authentication and access control • Software security • Physical security • Human resource security	Not applicable	Likely	Major	Extreme	2
Learning management system (LMS)	• Web/network security • User authentication and access control • Software security • Database security	Not applicable	Possible	Major	Extreme	3
Network channel/facility	• Web/network security • Physical security • Operation system security • Human resource security	Not applicable	Unlikely	Major	High	4
Mail system	• Web/network security • User authentication and access control • Human resource security • Operation system security	Not applicable	Likely	Moderate	High	5

4. Security Strategic

After the risk assessment, it is now to evaluate recommended control options. The risk register shows the vulnerabilities of the whole system clearly, and it is obvious that the risks could come from several same reasons/domains in these five key assets. By estimating different risks, we would concentrate on different domains in each key asset and give reasonable security controls with workable implement plans. All the controls are aimed at ensuring that the servers are deployed securely and remain secured against common automated and simple manual attacks.

4.1 Web/Application Servers and Databases Measurement Security Control

As the first important risk, web/application servers and databases serve as an important role in the whole system and therefore are vulnerable. Databases are the first and most important service provider as it replies to requests and responds patiently. In this system, databases work as a networked server and could be under network attacks. So, the first control is that the databases must never be directly exposed to the public, as Natan said in 2005. Because the databases could contain data of sensitivity, like the marks and scientific research. This requires the university to keep databases in the data center and protect it from external or internal attacks. Second, the university should have a group that is in charge of networking and databases at the same time. Otherwise, the database group may be not familiar with network technologies (like VLANs, routing tables) and the network group is not clear about access requirements. This could lead to ignorance between them, then it leads to terrible results. So the group should be aware of the nodes which the databases connect to and the data access diagram to maintain the right access control. Third, make sure to shut down superfluous ports and networked services because this can be used by hackers to break into the system. The networking and database group should make full use of two tools: Netstat and Nmap. Netstat could be operated on all operating systems and display current TCP/IP connections. Nmap is one of the most popular ports scanning tools and it monitors what the service is and whether it is run on a specific port by sending and receiving messages to each port. By using port scanners, the database could be more difficult to be attacked. Of course, some specific training is required to hoist the related capacity of the networking and database group. And relevant rules about using port scanning tools should be raised. Fourth, a SQL firewall should be used. In this way, policies can be set about IP addresses, ports, database users, database objects, SQL commands, and application types. By using a SQL firewall, the access to the database is limited, hence keep the security of the system. Fifth, define the standard to detect and monitor Distribute DOS to protect the availability of network security. The Chief Digital Officer should formulate related regulations and make it available to all students and staff. Sixth, the Chief Digital Officer should set up policies of using databases, illegal operations like modifying schema and tables should be strictly prohibited. Seventh, any operations to servers should be in conformity with relative policy and recorded. Eighth, make sure only administrators have the privileges to create, alter, or drop database users. Ninth,

physical protection for disasters like fire, flood, earthquake, explosion, civil unrest, and other forms of natural and man-made damage should be designed and applied. Tenth, information systems should be protected from power failure. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

4.2 Learning Management System (LMS) Security Control

During this tough period, the distance education becomes a more valuable and irreplaceable method of education. Also, how to identify a student correctly come into the necessity to avoid fraud. For Remarkable University, it is important to set up a valid authentication mechanism to get students correctly assessed, identified, and authenticated. First, for the mostly used username/password mechanism, some policies must be formulated by the Chief Digital Officer. Use at least one special symbol and capital form in the password. Short phrases/sentences are recommended. The password should be at least 12 places and should pass the proactive password checking. Username and password sharing is prohibited. And using the same password across different systems is discouraged. The Chief Digital Officer should ask students to change passwords every trimester. With these regulations, it is difficult for hackers to crack the password. Second, some biometric methods could be used during authentication to build up a more accurate and reliable security system. Considering the cost, it could be used on some specific occasions like exams and assignments. To reach a balance between accuracy and cost, face recognition could be a good choice with the advantages of convenience and effectiveness (Farshchi & Toosizadeh, 2011). As for cross-site scripting (XSS), it is a complex problem and could not be resolved in one step. But with caution, some procedures can be used to deal with it. First, input filtering is a basic tactic which is commonly used in this situation. Input filtering contains two parts: input blocking and input sanitation but note that each of these methods is fraught with risks and should be thoroughly understood before implementation (Grossman, Hansen, Petkov, & Rager, 2007). Thus, appropriate training is considerable. Second, JavaScriptbased extension could be a better solution. In 2018 Jamwal and Sharma claimed that "···has two units: Detection Unit and Action Unit. Detection unit follows pre-defined steps to detect the presence or absence of the attack and the action unit takes certain actions to successfully mitigate the attack" (Jamwal & Sharma, 2018, p. 3737). SQL attack is one of the most utilized web attack vectors, by this way hackers can get sensitive data from organizations. First, a valid counteract is to control and vet user input to watch for attack patterns. Second, vulnerabilities could also be avoided if developers can care about input validation, parameterized queries, stored procedures and escaping. Third, the SQL firewall should be used to lift the security of databases. Fourth, the Chief Digital Officer should take feedback about the service condition of the system from users periodically.

4.3 Network Channel and Facility Security Control

Denial of Service (DOS) attacks are one kind of attack to disrupt legitimate users' access to services. But there are some counteracts for Remarkable University to avoid it: involve in more nodes in the Internet to detect and respond to DOS; the service providers cooperate among key defensive points; use more reliable mechanisms to authenticate the resource of Internet traffic; trust the collaboration among distributed components (Zargar, Joshi, & Tipper, 2013). The network channel and facility can be affected by physical security like environmental, technical, and human-caused threats. So physical security is an essential part of the whole system to form a solid basic for all other security efforts. The policy should be clear to all the users and all the changes and new releases should be available to them as soon as possible (preteshbiswas, 2020). First, a list of personnel with authorized access to the facilities should be kept and reviewed by authorized personnel periodically. Security perimeters should be developed to protect the information system. Physical access to the server areas must be controlled and servers shall be kept in the server racks under lock and key. Access to the servers must be restricted only to designated Systems and Operations Personnel. Physical access to the information systems shall be monitored to detect and respond to physical security incidents. The access records of the visitors shall be maintained. This can prevent unauthorized physical access, damage, and interference. Second, physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural and man-made disasters shall be designed and applied. Third, information systems shall be protected from power failure and other disruptions caused by failures in supporting utilities. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage (preteshbiswas, 2020). Human resources are also critical for data security considering risks from intentional or unintentional behaviours of users. To avoid these situations, firstly the Remarkable University should provide data security training for HR team, tutors and students. Secondly, the Chief Digital Officer should enforce policy and encourage accountability for users. The network device is the basic of higher level of service, it is necessary to define a proper standard for each kind of device and also the conventions of usage of them. Note that periodic maintenance is the key to keep the whole system in a healthy condition.

4.4 Mail System Security Control

Mail system is a commonly used application in daily life and also would be a powerful tool in this system. To ensure that students and staff understand the limitation of using university account mail, policies should be available to them to protect data from breaches and safeguard the university's reputation and technological property (Corporate email usage policy template (Workable, 2020). First, with the account from the university, the students and staff should care about the reputation: never sign up for illegal, unreliable, disreputable, or suspect websites and services; never send unauthorized marketing content or solicitation emails; never send insulting or discriminatory messages and content; never intentionally spam other people's emails,

including their co-workers. Second, email is often the medium of hacker attacks, viruses and other malware. To protect the students and staff, they should: avoid opening attachments and clicking on links when content is not adequately explained; be suspicious of clickbait titles; check email and names of unknown senders to ensure they are legitimate; look for inconsistencies or style red flags. Third, by using some security options to improve mail security: use anti-virus/phishing/spam scanning; set attachment blocking; limit attachment size. Fourth, because the mail account comes from Remarkable University, there exists a relationship between the university account and mail account. Whenever a breach detected, passwords for both accounts can be considered unsafe and should be changed immediately. To track the history of mails and improve the mail system, electronic messages must remain accessible while they are required to meet. An appropriate signature (your name, position, and name of organisation) should be included in the tail of the official mails. Retain the transmission data of official mails to ensure the integrity of the email as recorded, for instance, the date and time of the message, sender. Also, proper training should be provided to users to maintain the mail system security at a high level.

4.5 Security Implementation Plan

The detailed of security strategy has been shown in Table 3 below:

Table3: security strategy

Assets	Level of Risk	Recommended Controls	Selected Controls
Web/application servers and Databases	Extreme	• database not directly exposed to the public • use the same group in database and networking • use SQL firewall • detect and monitor Distribute DOS • set up policies of using database • operations to servers should be recorded • only administrators have specific privileges • physical protection against physical damage should be designed • systems should be protected from power failure	• use the same group in database and networking • shut down superfluous ports and networked services and use the two tools
Learning management system (LMS)	Extreme	• biometric method • JavaScriptbased extension • control and vet user input • developers care about prevention methods • use SQL firewall • get feedback from users periodically	• input filtering • formulate policies on username/password mechanism
Network channel/facility	High	• counteracts to environmental threats • counteracts to technical threats • counteracts to DOS • provide data security training • enforce policy and encourage accountability • define a standard for network devices • periodic maintenance	• counteracts to human-caused threat
Mail system	High	• security options • password relationship between accounts • electronic messages must remain accessible • add an appropriate signature • retain the transmission data • provide proper training	• ‘never-do’ list to protect the reputation • ‘should-do’ list to protect students/staff

5. Implementation

IT security plan does not end with the security strategic as there are some risks that have not identified leaving the Remarkable University IT security system remains vulnerable. Therefore, this section is also crucial because without it there are chances that other safeguards and policies will not be deployed effectively.

First, the hidden risks may include the new unknown viruses, the invention of quantum computers, and the disgruntled users (administrative staff, tutors, and students). Second, the security strategy could not totally avoid the risks above. The threat to the system will never end because of different reasons (trick/malicious attack/unintentional), and it is a never-ending battle between attackers and countermeasures. When there are new countermeasures, there might be new attacks to bypass them. Hence, thirdly old policies and regulations could be unfitting to the current condition.

Considering the change of personnel (student graduation/enrolment), the Remarkable University should provide training to users/staff/students periodically and update relevant policies accordingly. The network servers and devices also need scheduled maintenance/replacement by the Chief Digital Officer.

Reference:

Alipour, S., Arabani, S. G., Asadi, M. T., & Zareii, R. (2013). Importance of planning and control of managers. Journal of Business and Management. 2(9). 36-38. Retrieved from https://pdfs.semanticscholar.org/f070/5371327312603173f0 b4a55255b9 83f5f792.pdf

Barik, N., & Karforma, S. (2012). Risks and remedies in e-learning system. *International Journal of Network Security & Its Applications (IJNSA). 4*(1). 51-59. doi: 10.5121/ijnsa.2012.4105

Farshchi, S. M. R., & Toosizadeh, S. (2011). A safe authentication system for distance education. *Computer Applications in Engineering Education. 22*(4). 593-603. doi: 10.1002/cae.20583

Grossman, J., Hansen, R., Petkov, P. D., & Rager, A. (2007). *XSS Exploits.* Burlington, Mass: Syngress.

Jamwal, K., & Sharma, L. S. (2018). Clickjacking attack: Hijacking user's click. *International Journal of Advanced Networking Applications. 10*(01). 3735-3740. doi: 10.35444/IJANA.2018.100110

Kumar, S., & Dutta, K. (2011). Investigation on security in LMS Moodle. *International Journal of Information Technology and Knowledge Management. 4*(1). 233-238. Retrieved from http://www.csjournals.com/IJITKM/PDF%204-1/47.pdf

Natan, R. B. (2005). *Implementing database security and auditing : a guide for DBA's, information security administrators and auditors.* Burlington, USA: Elsevier Inc.

Preteshbiswas. (2020). *Example of physical security policy*. Retrieved from https://isoconsultantkuwait.com/2020/02/01/example-of-physical-security-policy/

Queensland Government. (2020). *QGEA policies, standards and guidelines*. Retrieved from https://www.qgcio.qld.gov.au/publications/qgea-policies,-standards-and-guidelines

Reimer, B., Simpson, D., Hajer, J., & Loxley, J. (2009). The importance of policy for community economic development. Retrieved from http://ec.msvu.ca/xmlui

/bitstream/handle/10587/576/ManitobaPolicyPaper.pdf?sequence=1&isAllowed=y

Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice* (3rd ed.). London, UK: Pearson Education.

Ufartiene, L. J. (2014). Importance of planning in management developing organization. Journal of Advanced Management Science, 2(3), 176-180. doi: 10.12720/joams.2.3.176-180

Workable. (2020). *Corporate email usage policy template.* Retrieved from https://resources.workable.com/email-usage-policy-template#

Zargar, S., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials. 15*(4). 2046-2069. doi: 10.1109/SURV.2013.031413.00127

Revision History

The table 4 below detail about the procedures to complete this assignment in term of date of change, contributor, and summary of change.

Table4: Revision History

Date of Change	Contributor	Summary of Change
22-08-2020	Heang Sok_s5204340, Jingdi Lin_s5210032	• The group were formed • First group discussion at Gold Coast campus, Building: G30 • Responsibilities: +Heang Sok worked on introduction, key IT assets, and risk assessment +Jingdi Lin worked on security strategic and implementation
24-08-2020	Heang Sok_s5204340	• Completed key IT assets and risk assessment and sent to Mr. Jingdi Lin
26-08-2020	Heang Sok_s5204340, Jingdi Lin_s5210032	• Second group discussion at Gold Coast campus, Building: G30 • Further discussion on Key IT assets and risk assessment • Discussed on security strategic and implementation • Conclusion: +Mr. Heang Sok needed to make a few amendment on key IT assets and risk assessment
28-08-2020	Heang Sok_s5204340	• Completed the introduction and revised on key IT assets and risk assessment and sent it to Mr. Jindi Lin
29-08-2020	Jingdi Lin_s5210032	• Completed security strategic and implementation and sent to Mr. Heang Sok
05-09-2020	Heang Sok_s5204340, Jingdi Lin_s5210032	• Third group meeting at Gold Coast campus, Building: G30 • Further discussion on each part again • Combine each part together and check the formats, grammars, spellings, and referencing.
06-09-2020	Jingdi Lin_s5210032	• Perform final check, and submit the assignment