|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name | Amir Mahdi Sarikhani Fard | Student Number | | 474807620 |
| Unit Code/s & Name/s | BSBINS401 Analyse and present research information  ICTICT443 Work collaboratively in the ICT industry | | | |
| Cluster Name  *If applicable* | Cyber Research Cluster | | | |
| Assessment Name | Cyber Research Portfolio | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | Date submitted | | 28 / 11 /2024 |
| Assessor Name |  | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | |
| Student Signature | Amirmahdi Sarikhanifard | | Date | 28 / 11 /2024 |

|  |  |
| --- | --- |
| **Instructions to Student** | **General Instructions:**  You are employed by Midtown IT as a Cyber Consultant. You have been assigned to a new project, and your task is to research and report on current cyber safety and communication practices for virtual collaborative environments. In addition, you need to develop two related protocols for the organisation.  Your teacher/assessor will take on the role of the Project Manager assigned to this project by Midtown IT.  Read the project documentation provided and familiarise yourself with the Project Scenario or Case Study before proceeding with portfolio tasks. Confirm anything you are not sure about the project with your manager (teacher/assessor). It is essential that you have a clear understanding of the scenario and tasks that you need to complete. |

|  |  |
| --- | --- |
|  | This assessment instrument requires the student to complete a project portfolio that is divided into four (4) parts:  **PART 1 – Identifying research strategy and collecting research data**  Task 1 Identify research strategy and sources  Task 2 Collecting and storing research information  **PART 2 – Analysing and synthesising research data**  **PART 3 – Presenting research findings**  **PART 4 – Identifying team protocols requirements**  TASK 1 Cyber safety protocol and virtual meetings protocol  TASK 2 Virtual collaboration tools  TASK 3 Reviewing selected technologies  TASK 4 Review protocols compliance  TASK 5 Collecting and replying to feedback  **Materials to be supplied:**  You are required to provide your own storage device.  **Assessor to Provide:**  Access to PCs and peripherals – these may differ between classrooms  Access to the internet  Access to Connect (LMS)  Access to Word processing software, such as Microsoft Word  Access to special purpose tools, equipment, and materials to complete the assessment, for example diagramming software.  **Online Delivery**  Students to supply their own PC or laptop and peripherals and internet access  Students will require access to Microsoft Office or similar application  **Documentation:**  Midtown IT Scenario or Case Study  Midtown IT Collection, Storage and Reporting of Research Information procedure. |

|  |  |
| --- | --- |
|  | **Assessment Criteria:**  To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard. Demonstrated ability to:  Understand research objective  Select a suitable research strategy  Collect, store and share research information  Analyse and synthesise research information  Identify patterns and trends  Draw and justify research conclusions  Prepare and present research findings  Develop at least two protocols for teams working collaboratively in virtual environments that help achieve team objectives  Identify at least two communication tools and technology to support teams working collaboratively in virtual environments  Review compliance of protocols to work collaboratively in a virtual environment  Seek and respond to feedback  Share knowledge and information according to work details, team objectives, organisational policies and procedures  Refer to the marking criteria for specific details:  Cyber research cluster\_AT2\_MC\_TQM\_v1.  **Details of location:**  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  **Time restrictions:**  This assignment is designed to take place over 8 weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to 3 hours per week of their own time to study or study-related activities. |

|  |  |
| --- | --- |
|  | **Interactions:**  Teamwork skills are essential in the IT industry. Therefore, you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Level of assistance permitted:**  Staff cannot directly show students answers or solutions but can support and guide them to complete tasks individually. Teachers and tutors should be available in class and accessible by email for students working from home.  **Reasonable Adjustments:**  Reasonable adjustments are available to students for a variety of reasons, including disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  **Number of Attempts:**  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections/questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  ***For more information, refer to the Student Rules.***  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT-related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Submission details** (if relevant) | **Evidence Required to be Submitted:**  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission. |

|  |  |
| --- | --- |
|  | **Submission via Connect:**  Upload a single file into Assessment 2 (AT2) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  Name the file:  BSBINS401\_ICTICT443\_AT2\_Surname\_Student Number  TAFE Queensland Learning Management System (Connect)  **Accessing Connect:**  Assessment to be submitted via   * TAFE Queensland Learning Management System (Connect): [*https://connect.tafeqld.edu.au/d2l/login*](https://connect.tafeqld.edu.au/d2l/login) * Username; 9 digit student number   For password resets go to: [*https://passwordreset.tafeqld.edu.au/default.aspx*](https://passwordreset.tafeqld.edu.au/default.aspx) |
| **Instructions to Assessor** | **Online Delivery:**  Please revise and modify the Instructions to Student section if you are delivering online.  **Specifications of assessment:**  To be judged competent in this assessment item, the student is required to demonstrate competence in all indicators shown in the marking guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the IT development fields of work and include access to:  Research tools  Project requirements  Ensure that students read and familiarise themselves with the Project Scenario and the files and resources provided before attempting the assessment.  **Storage Devices:**  Students are required to provide their own storage device. |

|  |  |
| --- | --- |
|  | **Assessor to Provide:**  Access to PCs and peripherals – these may differ between classrooms  Access to the internet  Access to Connect (LMS)  Access to Word processing software, such as Microsoft Word  Access to special purpose tools, equipment and materials to complete the assessment, for example diagramming software.  **Online Delivery:**  Student to supply their own PC or laptop and peripherals and internet access  Students will require access to Microsoft Office or similar application  **Documentation:**  Midtown IT Scenario or Case Study  Midtown IT Collection, Storage and Reporting of Research Information procedure.  **Level of Assistance Permitted:**  Teachers and tutors should be available in class and accessible by email for students working from home. Staff cannot directly show students answers but can support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  **Interactions:**  Teamwork skills are essential in the IT industry. Therefore, you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Contingencies:**  Reasonable adjustments are available to students for a variety of reasons, including disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. |

|  |  |
| --- | --- |
|  | **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT-related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Note to Student** | An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide. |

## PROJECT SCENARIO

Midtown IT ***WHS Consulting Department*** provides a wide range of services to industry and government. These services include:

* Risk management assessment
* Risk management control
* Risk management audit and performance
* Compliance and due diligence
* WHS legislative requirements

The company wants to take advantage of current communication and collaborative tools and will encourage staff in specific roles to work remotely. Although the company is keen to start immediately, management has identified that a number of protocols regarding online collaboration must be set in place.

All employees will be provided with the necessary equipment to work remotely. This includes PCs or laptops and high-quality web cameras.

The company objectives are:

* Improve the efficiency of team communication
* Provide safe and reliable professional channels for teams to communicate and share knowledge and information virtually

**THE TASK**

Your task is to carry out the necessary research to complete two company protocols. Details of the task requirements are presented below:

**Research requirements**

The aim of the research effort is to identify current practices in virtual and collaborative environments and use the information gathered to write the company protocols. The research requirements include two separate research topics:

1. Current industry cyber safety practices for virtual environments
2. Communication practices and techniques used in virtual collaborative environments

**Research objectives**

Midtown IT research objectives include:

* Measurable outcomes
* Currency of the research
* Reliability of sources
* Industry-accepted strategies, methods and tools included in the research

**Protocols development requirements**

Once the research component has been completed and appropriately stored and documented, Midtown IT requires you to develop two protocols to manage and guide the virtual communications and collaborative activities of the organisation. The protocols required are:

* Cyber Safety protocol
* Virtual Meetings protocol

## PART 1 – Identifying research strategy and collecting research data

The scenario requires you to research two (2) separate topics, but for the purpose of this portfolio, the preparation of the two topics can be presented together as they are related and share the research objectives.

Complete the activities listed in PART 1 for each research topic.

Task 1 Identify research strategy and sources

1. Carefully review the scenario presented until you have acquired a clear understanding of the research task. Outline and briefly describe the research objectives.

As mentioned, we are working in Midtown IT ***WHS Consulting Department,***  where we have interactions with industry and government. We provide different kind of services associated with Risk management, compliance, and WHS legislative requirements. There has been a trend in our organization recently encouraging staff to work remotely (in specific roles), leading our organization to focus on implement beneficiary advanced communication and collaborative tools. In this case, we have been assigned to set a few protocols regarding online collaboration based on the research prior to starting this change. It has been mentioned that will be equipped before starting working remotely. Company has stated that their objectives are about to enhancing the efficiency of team communication by establishing safe and professional channels where communication among teams can be undergone. In these channels, teams will be able to share knowledge and information virtually.

1. Identify the most suitable research strategy for the research scenario presented (e.g., qualitative, quantitative or combination) and justify your selection.

I do believe we need to use a combination of both qualitive, and quantitative research strategies based on the given scenario and outlined objectives. In order to understand practices and techniques, sometimes interviews (as an example) can provide us in depth insights into recent industry cyber safety practices and communication techniques used by staff. Sometimes there are opportunities in this kind of research which can’t be find in quantitative research. So, these interviews need to be conducted with employees from different companies we are affiliate with. In these interviews we will receive their valuable experience and suggestions on our virtual communication and collaboration, ensuring thar our protocols outcomes are friendly and meet user needs. For quantitative research method, we can collect information by surveys and data analysis, which can provide you with measurable outcomes and statical evidence requested. Quantitative methods can be beneficial as it allows us to evaluate performance and reliability of our communication and collaboration tools using numbers its holding in its data. Quantitative data also can help us in understanding of trends in the industry about virtual communication and collaboration tools.

1. Identify potential sources of information and assess the reliability of the sources for the two research topics. Include at least five (5) sources per topic. Use the table provided below to complete this activity.

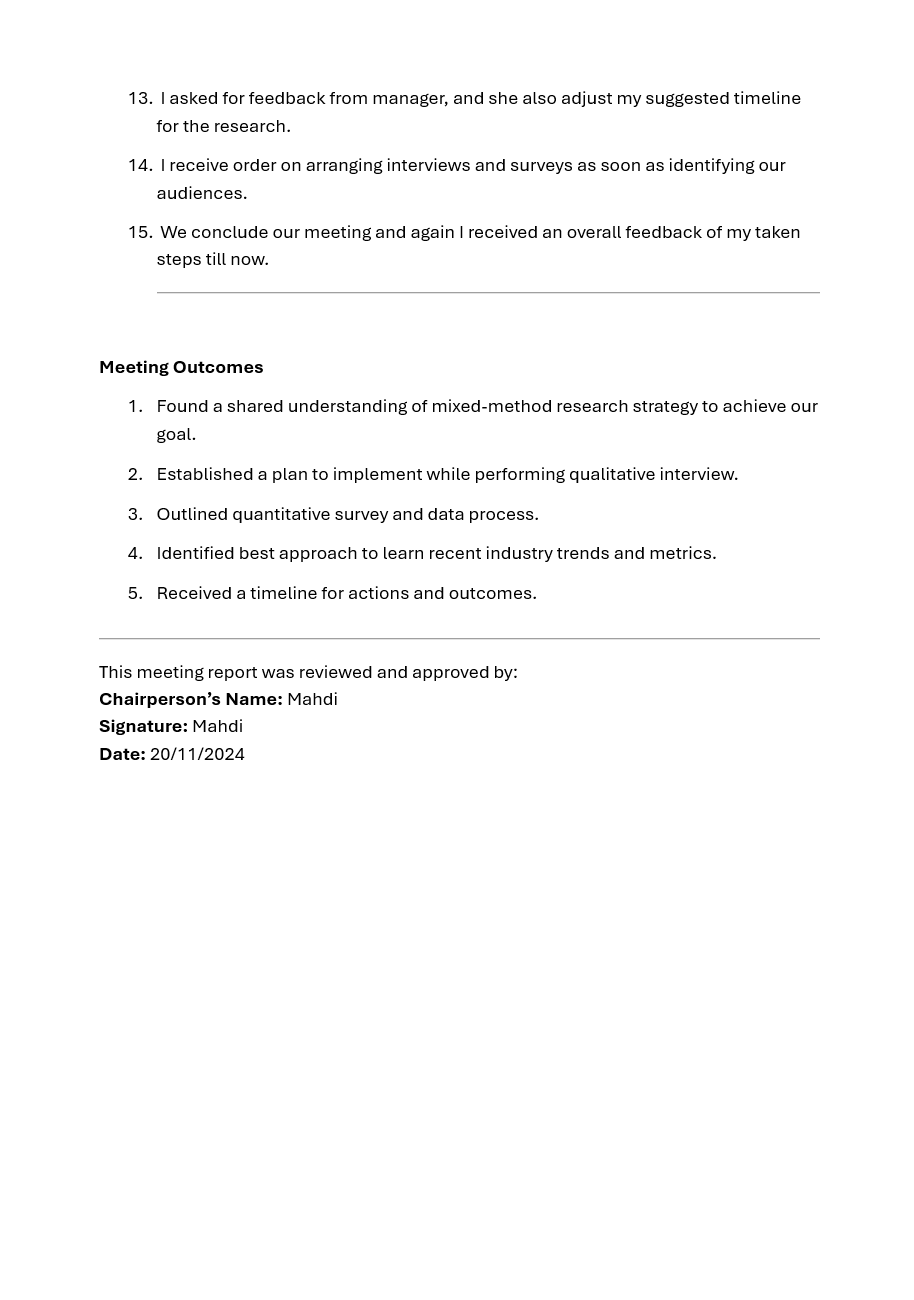
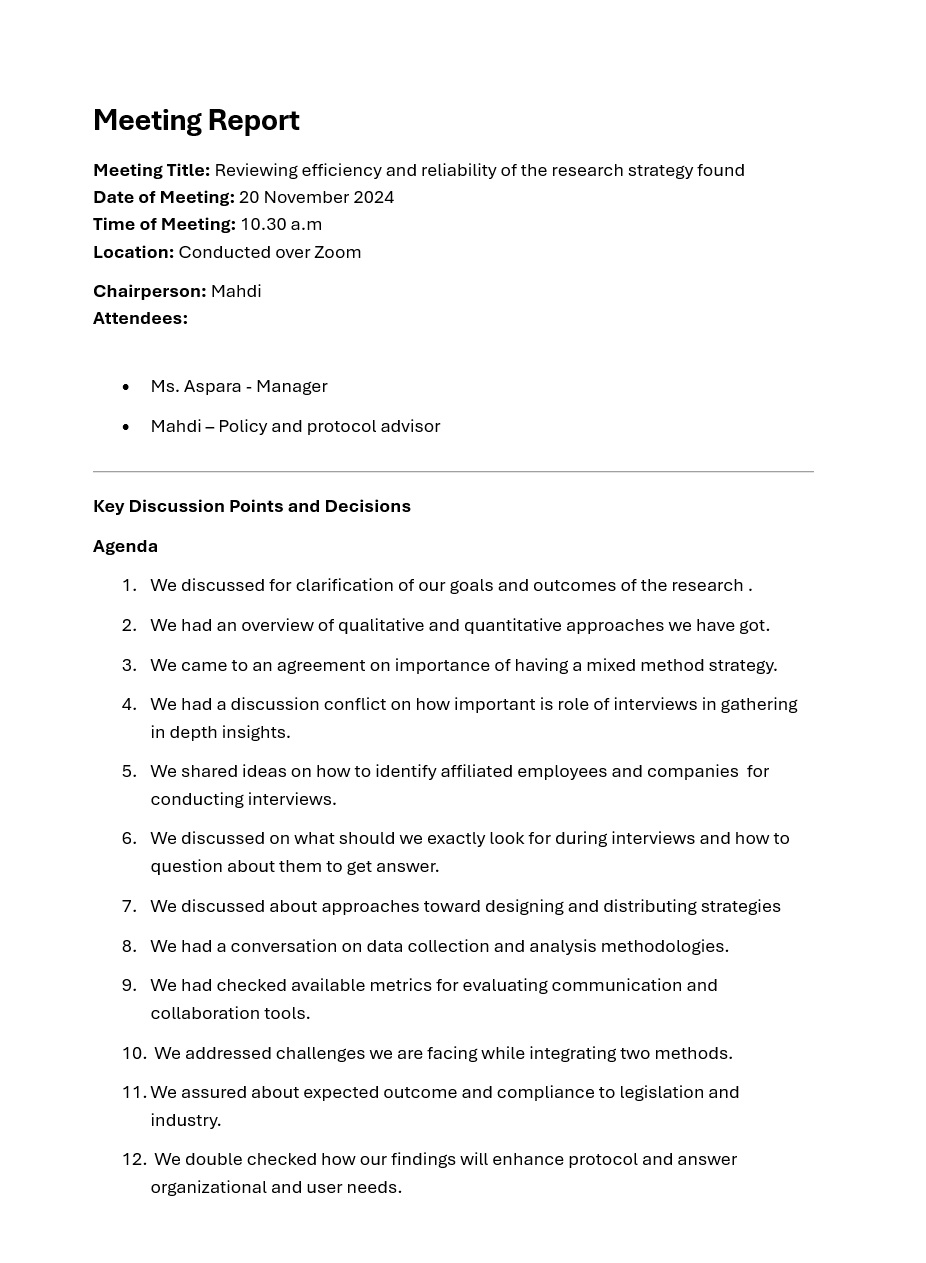
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Potential Sources** | **Reliability Criteria** | | | | |
| **Creator/Origin** | **Currency** | **Availability** | **Verifiable with secondary sources** | **Purpose** |
| Secure remote working practices | | | | | |
| [Remote working | Cyber.gov.au](https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/remote-working-and-secure-mobility/remote-working) | Australian Cyber Security Centre | Updated regularly | Publicly available  **Weblink** | Yes | Offers guidance on secure remote working |
| [Cyber safety: do your employees know how to stay safe online?](https://www.essentialtech.com.au/blog/cyber-safety-do-your-employees-know-how-to-stay-safe-online#:~:text=Ensuring%20your%20employees%20are%20aware%20of%20your%20security%20policies%20and,two%20ways%2C%20symmetric%20and%20asymmetric.) | Essential Tech | Recent  2 years old | Publicly available  **Weblink** | Yes | Provides advice on employee cyber safety |
| [Keep it Safe: A Guide to Cybersecurity in a Virtual Office](https://www.cm-alliance.com/cybersecurity-blog/keep-it-safe-a-guide-to-cybersecurity-in-a-virtual-office) | CM Alliance | Recent  2023 | Publicly available  **Weblink** | Yes | Outlines cybersecurity best practices |
| [Essential Eight | Cyber.gov.au](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight) | Australian Cyber Security Centre | Updated regularly | Publicly available  **Weblink** | Yes | Details essential cybersecurity strategies |
| [IT: The Key to Effective Work | Okta](https://www.okta.com/au/resources/whitepaper-it-the-key-to-effective-work/?utm_source=google&utm_campaign=apac_anz_mult_all_wf-all_dg-ao_a-wf_search_google_text_kw_SSO_utm2&utm_medium=cpc&utm_id=aNK4z000000UECQGA4&gad_source=1&gclid=EAIaIQobChMItsr8sb_piQMV5aNmAh0l1xt9EAAYASAAEgKhaPD_BwE) | OKTA | Recent  Not specified | Publicly available  **Weblink** | Yes | Shares best practices for remote work |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Virtual communication fundamentals | | | | | |
| [Improving Virtual Collaboration in Your Organization | CCL](https://www.ccl.org/articles/leading-effectively-articles/how-to-improve-your-organizations-virtual-collaboration/) | Centre for Creative Leadership | Recent  2022 | Publicly available  **Weblink** | Yes | Provides strategies for effective virtual collaboration |
| [11 Effective Ways To Support Enhanced Virtual Communication](https://www.forbes.com/councils/forbesbusinesscouncil/2021/10/20/11-effective-ways-to-support-enhanced-virtual-communication/) | Forbes Business Council | Recent  2021 -2022 | Publicly available  **Weblink** | Yes | Shares expert advice on virtual communication |
| [Virtual Team Communication: Best Practices to Work Better Together](https://fellow.app/blog/management/virtual-team-communication-best-practices/) | Fellow App | Recent  2021 -2022 | Publicly available  **Weblink** | Yes | Discusses best practices for virtual team communication |
| [17 Tips & Best Practices to Improve Virtual Team Collaboration](https://www.avocor.com/blog/virtual-team-collaboration/) | Various Industry Experts | Recent  Not specified | Publicly available  **Weblink** | Yes | Provides tips and best practices for virtual collaboration |
| [proviz-developer-pexip-success-story-2493227-r2-web.pdf](https://developer.download.nvidia.com/maxine/proviz-developer-pexip-success-story-2493227-r2-web.pdf) | NVIDIA Developer Blog | Recent  2022 | Publicly available  **Weblink** | Yes | Discusses innovative technologies for virtual meetings |
|  |  |  |  |  |  |

1. Discard unreliable sources after completing task 1.3. If necessary, add and assess new sources of information.

Checked, and everything seemed to be aligned with our expectations.

1. Arrange a meeting with your manager or relevant personnel to confirm the efficiency and reliability of the research strategy identified in 1.2 for the research objectives presented in the scenario. Document the meeting.



Task 2 Collecting and storing research information

1. Access the *Midtown IT Collection, Storage and Reporting of Research Information* procedure. The procedure includes the following sections:

* Research data ethics
* Storage during the research phase
* Sharing research data
* Storage after the research phase
* Securing research data
* Retention and disposal of research data

For this task, you need to:

1. Collect relevant research information from the sources identified in 1.3.

70 percent done qualitative data

1. Store and secure research information according to *Midtown IT Collection, Storage and Reporting of Research Information* procedure.

Stored \*

## PART 2 – Analysing and synthesising research data

**NOTE: Analysis** involvesbreaking down the information into simpler ideas. **Synthesis** involves combining the individual elements to form a new idea, usually presented in a single sentence.

The scenario requires you to research two (2) separate topics, but for the purpose of this portfolio, the analysis of the two topics can be presented together.

1. For each research topic, analyse and synthesise your stored research data according to the research strategy selected. Document the analysis and synthesis. As a minimum, you must use the five (5) steps presented in the table below.

|  |  |
| --- | --- |
| Analysing and Synthesising Research Data  Secure remote working practices | |
| Steps | Analysis and Synthesis |
| 1. Review research objectives | We are supposed to perform research on cyber safety (and partly communication techniques) to find the latest measures for virtual environments where we can attach discovered effective communication methods in virtual environment between teams. So our objectives needed to obey a series of defined merits such as being up to date, reliable, guaranteed measurable outcomes and compliant with accepted industry strategies. After research and data collection, we need to gather all together to conclude to cyber safety protocol along with a Virtual Meeting Protocol. |
| 1. Review research data organisation (e.g., themes, categories) | I have created a template for organizing my data collected which I do believed can be used to feed an analyser platform if we wanted to go further. In this template, I have dedicated two separate tables for each topic and created each one 10 columns which are Source title, Author(s), publication date, publisher/Journal Name, Link, Type of source, Relevance to Research, Notes /Observations and Citation. |
| 1. Discover patterns, themes, trends and practices | All of data collected from each website had similar pattern, but as we put them next to each other they have potential to structure a theme based on how they are organized. In path to completing this mentioned, we also faced trends. Below is a summary: **Key Patters and Themes**  1. Strong Emphasis on Account Security:  We have got multi-factor authentication which has been highlighted multiple times as critical measure to prevent unauthorized access while using our devices and accounts for virtual communication. Moreover, there are recommendations for creating and maintaining strong, unique passwords and passphrases are consistently suggested, including the use of passport management tools.  2. Device and Data security:  There are a series of suggestion and essential security tips associated with devices being used for virtual communication. Suggestions can be like locking devices when unattended, keeping software updated, and performing regular data backup. Further, we found suggestions about safeguarding against risks associated with external devices being used and shared among staffs. Moreover, there are good practice suggestions to be implemented while using cloud storage along with encryption transfer as an encouraged alternative secure file transfer and storying method.  3. Network Security  We found recommendations including secure connection practices while being connected to the Wi-Fi network such as altering default settings and also avoiding public Wi-fi unless necessary. In addition, there are emphasise on importance of VPN usage for secure connections while working remotely.  4. Awareness of Surroundings and Potential Scams:  In our data collection, we observed that they have been stating the need for individuals to be cautious about their surroundings when accessing sensitive information, they usually handle while they are communicating virtually in a remote working area prevent data breach. Moreover, there are awareness regarding scams and the techniques used by cybercriminals, including identity theft, phishing and more hazardous threats they may face. These awarenesses mentioned can help us enrich our practices for mitigating such threats.  5. Use of remote Desktop Client  There are lots of industry guidelines associated with secure configuration of remote desktop clients to mitigate risk we face with remote access. In this case, we have found data on leading our path in the handling sensitive data within remote sessions with organized guidance provided by industry and government’s frameworks.  6. Web Conferencing Security  We have also collected data associated with guidelines on how to select and implement web conferencing solutions where provider has got strong encryption practices, and the ability to accommodate privacy and legal requirements for its users. It gives recommendations on how to securely conduct meetings on such solutions. |
| 1. Summarise findings and recommendations | We were able to come to decision on usage of several key security practices those was highlighted in our collected data for virtual communication. In our data collected in last step, Account security was our priority which was almost main subjects of all of statements. In this case, we tried to address it with recommendations such as multi-factor authentication and implementing password management tools. We further decided to find a frame for our practices which was possible with having an understanding of our own device and data security industry requirement in framework they have presented. If we just want to state basic examples of advices can be possible outcome of our practices, we can state locking devices, updating software, and using encryption. Moreover, we decided to build a foundation which our employees can return to it for securing their connections. This will address their network security, where we can aid them in securing their Wi-Fi connections, asking them to prevent public network connections, and using VPNs for remote work. Lastly, we thought it is necessary to consider environmental elements and use data to tell them about importance of cyber awareness. This will help them in preventing including phishing attacks and identity theft. Finally, we came to conclusion that these data are acceptable for structuring best practices for securing clients, web conferencing tools and staffs. I do believe all these characters can aid each other to protect sensitive data and ensure privacy for each sides. |
| 1. Share and distribute findings | In order to share it within the organization, I do believe that we first need to review the if there are existing security policies in this organization, using which we can ensure compliant with any specific requirements or protocols we may have missed. Based on the findings, I can establish a communication plan as a foundation for all of future communication among employees where they can find clear guidelines and best practices. This can be along with formal training sessions and learning materials. I need to identify internal channels such as email, the company intranet or the company’s Model learning platform. Additionally, we may need some regular reminders along with updates which need to be sent to them, and lastly a feedback mechanism will be helpful when it comes to addressing questions and concerns. Using distribution process, I can ensure that all staff are aware of these practises and adhere to the updated security protocols. |
|  |  |

|  |  |
| --- | --- |
| Analysing and Synthesising Research Data  Virtual communication fundamentals | |
| Steps | Analysis and Synthesis |
| 1. Review research objectives | We are tasked with researching cyber safety and communication usual tips to identify the latest of them for virtual environments. Our aim is to find an understanding of effective communication methods between teams in these settings in virtual environment. Therefore, our objectives must adhere to several defined criteria, including currency, reliability, measurable outcomes, and compliance with accepted industry standards. Throughout our research and data collection, we will compile our findings to establish both a Cyber Safety Protocol and a Virtual Meeting Protocol. |
| 1. Review research data organisation (e.g., themes, categories) | I have been developing a template to organize the data collected. Using this template, I believe I can utilize it to enhance our efficiency for categorization where we will be enabled to perform analysis on our data. My template is featuring two tables, each one containing different topic of our research, each containing 10 columns: Source Title, Author(s), Publication Date, Publisher/Journal Name, Link, Type of Source, Relevance to Research, Notes/Observations, and Citation. I do believe that this structured approach is going to be helpful when dealing with the fundamental principles of virtual communication found in our data, ensuring about their clarity. |
| 1. Discover patterns, themes, trends and practices | When we had all of the data collected analysed, we had some expected patterns revealed. After observing these patterns, we can realize that they offer that there is a potential to contribute to enhancing of our virtual communication practices’ theme. Throughout this analysis, we also were able to identify trends. Below I have listed summary:  **Key Patterns and Themes**   1. Emphasis on Hybrid Work Models**:** There has been a trend towards hybrid work arrangements, which is evident, with a notable preference among employees (47%) for a blend of remote and in-office settings even after pandemic. Organizations are encouraged to work on the flexible work policies they have got to again allow talent to show up and enhance employee satisfaction along with their efficiency. When we provide them a secure area and the way they securely access devices and accounts for virtual communication, there will be no concerns anymore. 2. Importance of Technology in Communication: As mentioned before, when a company rely on digital tools, it is obvious that their communication methods will be transformed, making them operate in more efficient and convenient manner. It is not only their communication skilled which will be benefited, but they will also learn about keeping themselves, employees, employers and clients safe in a way which has just enabled by virtual communication. I do believe that our employees will have more safe mental environment when they learn how to handle their usual concerns about passwords creation and maintenance with password management tools, giving their mind more peace for allocating time on higher priority stuffs. 3. Need for Relationship Building**:** In our data, we found that we need to systemically import teamwork culture to operations as a vital component of successful virtual collaboration. As we found, there should have social events being held outside of work hours, in order to get staff engaged and built working relations. In this way, we can foster a sense of belonging among them. This may need more psychological research to integrate it with our practices. 4. Balancing Tasks and Relationships**:** After analysis, we found that reaching a point where we have efficient virtual collaboration, is only possible by adjusting a balance between managing tasks and fostering interpersonal connections. So, we know that, the company is always encouraged to concentrate on both, maintaining best practices and also keep environment a place for employees growth. 5. Enhancement of Communication Skills**:** In patterns, we found that strong communication skills employees may have had in in person, may come handy for effective virtual teamwork. But, it is easy to understand that when employees communicate behind the their devices, they may face their own communicational barriers, and this can be different based on age and other similar factors. I think we can allocate on-going training based on a model found called LACE model standing for Listen, Ask, Challenge and Establish Accountability. This will help us having better interactions, and observations we have usually on surroundings, which will further possibly lead to prevention of social engineering during virtual communication ( if training being provided in appropriate way. 6. **Challenges in Virtual Collaboration:** Key challenges like building trust and managing time zones still persist in remote environments. Structured check-ins, project management tools for transparency, and regular data backups are essential strategies to mitigate these challenges, ensuring effective collaboration while maintaining device security. 7. **Focus on Engagement and Participation:** There’s a growing trend towards making virtual meetings more engaging. Utilizing polling, breakout rooms, and interactive content can enhance involvement, reinforcing our guidelines on secure web conferencing practices that prioritize user privacy and legal requirements. 8. **Best Practices for Virtual Meetings:** Effective meetings in remote settings are crucial. Following set agendas, minimizing attendees, and utilizing reliable technology are essential strategies that echo our findings on safeguarding communication channels, particularly during web conferencing. 9. **Tracking Results Rather Than Time:** The movement towards focusing on deliverables rather than traditional time-tracking is evident. Managers should set clear goals, emphasizing outcomes over hours worked while aligning this approach with our established guidelines on securing access and data integrity in remote communications. 10. **Creating Structured Communication Plans:** Clarity in virtual communication processes helps prevent misunderstandings. Developing a structured communication plan that designates appropriate tools for specific scenarios complements the recommendations for network security, including secure connection practices to mitigate risks in remote work scenarios. |
| 1. Summarise findings and recommendations | We were able to make key decisions regarding enhancement of virtual communication, based on the data we collected. Communication was highlighted as an element which can affect account security also. As a result, we decided not only focusing on multi-factor authentication but also make employees being able to safeguard their security while communicating. We also recognized the importance of importing best communications into our practices by using collected industry standards in our data, assuring that employees adhere to essential guidelines for safe communication.  The data also highlighted the need to holding ongoing training sessions to learn about these practices.  These practices will help us having a framework for our communication, ensuring that all communication between employees or stakeholders will remains safe. |
| 1. Share and distribute findings | In order to share it within the organization, I do believe that we first need to review the if there are existing conversation policies or code of practices in this organization, using which we can ensure compliant of our new one with any specific requirements or protocols we may have missed. Based on the discoveries, I can now establish a communication plan as a foundation for all of future communication among employees where they can find clear guidelines and best practices for communication. This hopefully can be presented along with ongoing training sessions during their work and learning materials in learning models. I need to discover internal channels such as email, the company intranet or the company’s Model learning platform. Additionally, we may need some daily or weekly basis reminders along with updates which are necessary to be sent to them ( in order to keep them updated), and lastly a feedback mechanism will be necessary when it comes to addressing future questions and concerns. Using mentioned process, I can assure that all employees are aware of these practises while operating remotely and obey to the updated communication protocols. |
|  |  |

1. For each research topic, identify and explain any recurring themes or practices in the research data (Step 3 above). Draw conclusions according to the research strategy utilised. Ensure that conclusions made are clear, justified and supported by the evidence collected during the research phase.

No Answer needed here

1. For each research topic, outline any assumptions made in the analysis. Justify their inclusion in the analysis in accordance with the evidence collected and the research strategy utilised.

Topic 1:

First, we assume that Industry Guidelines we have found are relevant. We further assumed that they are latest guidelines on cybersecurity we have got, such as authentication methods, device security settings recommended, and network protection advice. Then we assume that we will be able to have our employee’s engagement, and they will follow the defined security protocols if properly communicated through training and clear guidelines we will provide. This assumption was made based on the understanding we found after shaping structured communication and providing ongoing support would encourage them to adherence.

Lastly, we had some assumptions about technological compatibility, and we checked that the organization’s current technological infrastructure could support the utilizing of security setting I probably going to write in protocols.

Topic 2:

First, we assumed that combination of remote and in-office work, would continue to be helpful. This is supported by the evidence that many of our employees told us on survey that they prefer flexible work arrangements even when there is no pandemic.

We also assumed that our platforms communication and other learning technologies are ready.So, we first had an analysis using which I assumed that the organization would be the technologically ready and have up to date infrastructure to support the recommended communication tools and practices.

Lastly, we assumed that we would have employee engagement with training which will be provided and we thought we can encourage them to be active in ongoing training and learning of communication strategies which we will provide them.

## PART 3 – Presenting research findings

Complete the activities listed in PART 3 for each research topic.

**This section must be completed according to the Midtown IT Collection, Storage and Reporting of Research Information procedure. Access the procedure and follow the instructions and templates.**

1. List and briefly describe the agreed methods to share and report research information across the organisation.

1. Internal Communication Channels:

We came to decision to use email, the company intranet, or a learning platform we have got or we are developing to share research findings and updates.

2. Training and Learning Materials:

We are aiming to provide training sessions and sharing others learning materials to train staff after research to lead them toward best practices.

3. Regular Updates and Reminders:

We thought we need to broadcast updates and reminders through channels mentioned for keeping employees informed about ongoing developments causing changes.

4. Feedback Mechanism:

We thought we need to utilize a system to collect and address employee questions, suggestions, and concerns about the research information shared.

5. Research Reports and Presentations:

Lastly, We thought we can share our findings using structured research reports (by developing a standard template) and presentations, assuring clarity and compliance with data protection guidelines.

1. Prepare a research draft report using the template provided according to organisational procedures.

Nothing to submit

1. Present the research draft to the manager or relevant personnel for review and discussion. Document the discussion.
2. Amend the report as needed and prepare a final research report.
3. Present final report to manager seeking feedback and confirmation of the suitability and the findings.
4. Amend as needed and distribute the research report according to organisational procedures.
5. **Contingency task.** Assume that after the meeting with the manager (3.3), it is identified that a key research question has not been addressed by the research and no data has been collected. How would you rectify the omission?

If a key research question has been identified as unaddressed and no data has been collected for it, the following steps would be taken to rectify the omission:

1. **Reassess Research Objectives**
   * + Convene a meeting with the research team to evaluate the omitted question's relevance and urgency in relation to the research objectives.
     + Identify how the question aligns with the broader scope of the research and prioritize it accordingly.
2. **Develop a Revised Research Plan**
   * + Create a targeted plan specifically to address the missing question, including clear objectives, data requirements, and timelines.
     + Allocate additional resources, if necessary, to ensure the plan's swift implementation.
3. **Collect Missing Data**
   * + Use appropriate methods such as surveys, interviews, or additional literature reviews to gather data relevant to the missing question.
     + Ensure that data collection aligns with the standards and methodologies already established in the initial research.
4. **Analyze and Integrate Findings**
   * + Analyze the newly collected data and incorporate it into the existing research framework.
     + Cross-check how the new findings impact or refine previously established conclusions and recommendations.
5. **Communicate with Stakeholders**
   * + Update the manager and other stakeholders about the omission, the steps taken to address it, and the expected outcomes.
     + Present a revised timeline to accommodate the additional work required.
6. **Prevent Future Omissions**
   * + Evaluate the research process to identify how the question was missed and implement measures such as a more thorough planning phase or stakeholder reviews to prevent similar oversights in future projects.

## PART 4 – Identifying team protocols requirements

**TASK 1 Cyber safety protocol and virtual meetings protocol**

1. Using the information obtained during the research phase of the portfolio, you must write two (2) protocols to guide the virtual communications and collaborative activities of the organisation as identified in the scenario presented.

Use the forms provided below as they are part of Midtown IT organisational documentation procedures.

The required protocols are:

1. Cyber Safety protocol

|  |  |  |
| --- | --- | --- |
| Cyber Safety Protocol | | |
| **Protocol Rules** | **Who is Responsible? (Role)** | **Responsibilities** |
| Ensure strong passwords and enable multi-factor authentication (MFA). | |  | | --- | | IT Administrator |  |  | | --- | |  | | Configure MFA systems and monitor password policies. |
| |  | | --- | | Keep all software and devices updated. |  |  | | --- | |  | | |  | | --- | | IT Administrator | | Implement regular updates and security patches. |
| |  | | --- | | Use VPNs for remote work and secure network access. |  |  | | --- | |  | | IT Team | Manage and maintain VPN systems for employees. |
| Avoid public Wi-Fi and enable secure connections. | All Employees | Follow guidelines for secure internet usage. |
| Encrypt sensitive data during storage and transfer. | IT Administrator and Employees | Ensure encryption tools are used for critical data. |
| Educate staff on phishing and scam awareness. | HR and IT Team | Conduct regular cybersecurity awareness training. |
|  |  |  |
| Are the rules of this protocol aligned with work details, team objectives, organisational policies and procedures? | | |
| Yes  No | | |
| What type of knowledge is shared within the context of this protocol? | | |
| Guidance on secure password management, safe internet practices, phishing awareness, encryption techniques, and secure device handling. | | |

1. Virtual Meetings protocol

|  |  |  |
| --- | --- | --- |
| Virtual Meetings Protocol | | |
| **Protocol Rules** | **Who is Responsible? (Role)** | **Responsibilities** |
| |  | | --- | | Use only approved video conferencing tools. | | |  | | --- | | IT Team | | |  | | --- | | Provide and manage secure conferencing platforms. | |
| |  | | --- | | Configure meeting settings to require a password. | | |  | | --- | | Meeting Host | | |  | | --- | | Enable passwords for all virtual meetings. | |
| |  | | --- | | Limit screen sharing to the host unless necessary. | | |  | | --- | | Meeting Host | | |  | | --- | | Manage screen-sharing permissions. | |
| |  | | --- | | Avoid sharing sensitive information in public chats. | | |  | | --- | | All Participants | | |  | | --- | | Ensure chats adhere to confidentiality policies. | |
| |  | | --- | | Record meetings only when essential and permitted. | | |  | | --- | | Meeting Host | | |  | | --- | | Inform participants and store recordings securely. | |
| |  | | --- | | Follow a structured meeting agenda. | | Meeting Coordinator/Host | |  | | --- | | Distribute and adhere to the agenda to stay focused. | |
| Are the rules of this protocol aligned with work details, team objectives, organisational policies and procedures? | | |
| Yes  No | | |
| What type of knowledge is shared within the context of this protocol? | | |
| Information about secure meeting practices, confidentiality, and collaboration strategies to ensure effective and safe virtual communication. | | |

TASK 2 Virtual collaboration tools

1. You must research and identify two (2) industry standard suitable virtual communication and collaborative platforms or tools that Midtown IT could use for online activities and remote work.

Complete each section of the table.

1. Use the internet to research the collaborative platforms/applications
2. Use the table below to present your research

|  |  |  |  |
| --- | --- | --- | --- |
| Communication Collaborative Tool | Communication Techniques Supported | Advantages | Disadvantages |
| Microsoft Teams | |  | | --- | | Video conferencing, audio calls, chat messaging, file sharing, integration with Office 365 apps. |  |  | | --- | |  | | - Seamless integration with Microsoft Office tools. - Offers robust security and compliance features. - Allows real-time collaboration. | - Requires Microsoft 365 subscription. - Can be overwhelming for new users due to multiple features. |
| ZOOM | |  | | --- | | Video and audio conferencing, webinar hosting, screen sharing, breakout rooms, chat messaging. |  |  | | --- | |  | | - Easy to use with a user-friendly interface. - High-quality video and audio. - Supports large group meetings | - Free version limits meeting duration for groups. - Security concerns in the past, though improved. |

1. Provide references for all your sources. Use a formal referencing style such as Harvard or APA.

Microsoft. (n.d.). *Microsoft Teams*. Retrieved from <https://www.microsoft.com/en/microsoft-teams>

Zoom Video Communications, Inc. (n.d.). *Zoom Features*. Retrieved from <https://zoom.us/features>

Johnson, R. (2022). *A comparison of Microsoft Teams and Zoom for remote collaboration*. *Tech Journal*, 14(3), 45-52.

TASK 3 Reviewing selected technologies

1. Midtown IT requires you to create a checklist to review the technologies selected in 4.2. Use the table below. Complete each section of the table.

Once the comparison table is completed, mail the manager or relevant personnel and communicate the results of the comparison of the two (2) technologies.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Review Criteria | Microsoft Teams | Comments | ZOOM | Comments |
| Fit for purpose | Yes  No  Partially | Microsoft Teams may not support all our organization requirements or scenarios for small-scale virtual meetings. | Yes  No  Partially | |  | | --- | | Zoom is used for various purposes, including webinars, training, and small or bigger virtual meetings. |  |  | | --- | |  | |
| Reliable | Yes  No  Partially | Teams offers can higher reliability with strong integration using Microsoft’s base features, ensuring their efficiency. | Yes  No  Partially | Zoom is always providing stable connections mostly for larger meetings, instead they put issues with video quality or lags in small ones those can arise. |
| Efficient | Yes  No  Partially | Integrated tools for collaboration (file sharing, calendar) those improve efficiency. | Yes  No  Partially | It has got simple interface and efficient performance, though lacks advanced integration with productivity tools like Teams. |
| Compatible with existing systems | Yes  No  Partially | It is able to work seamlessly with current Microsoft 365 basics, which may already be implemented in organization. | Yes  No  Partially | Compatibility might be an issue if the company relies heavily on other productivity suites, requiring additional integrations. |
| Ease of use | Yes  No  Partially | It is user-friendly for individuals those who are familiar with Microsoft apps, but the learning it can be timetaking for new users. | Yes  No  Partially | Intuitive and simple interface; widely accepted as beginner-friendly for virtual meetings and webinars. |
| Aligns with company policies and procedures | Yes  No  Partially | It has been supporting its users with strict security, compliance, and privacy policies required in organizational settings. | Yes  No  Partially | It is providing encryption and compliance options, where our policies may need additional customization to meet all organization’s standards. |
| Team objectives | Yes  No  Partially | It encourages collaboration through enabling working with shared documents, task tracking, and integrated messaging tools in it. | Yes  No  Partially | It can enable us to have effective communication, but its focus on meetings its self rather than team collaboration. |

**Task 4 Reviewing protocols compliance**

1. Midtown IT also requires you to create a checklist to review the compliance of the protocols written in PART 4 - Task1. Complete each section of the tables.
2. Cyber Safety protocol checklist

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cyber Safety Protocol Review Form | | | | |
| Rules | Full Compliance | Minor Non-Compliance | Major Non-Compliance | Suggested Improvements (If Necessary) |
| Ensure strong passwords and enable multi-factor authentication (MFA). |  |  |  | Conducting periodic training on password creation and MFA activation. |
| Keep all software and devices updated. |  |  |  | Automating software updates and notify teams about critical updates. |
| Use VPNs for remote work and secure network access. |  |  |  | Providing employees with clear VPN setup guides and technical support. |
| Avoid public Wi-Fi and enable secure connections. |  |  |  | Providing portable secure hotspots and educating teams on secure practices. |
| Encrypt sensitive data during storage and transfer. |  |  |  | Reviewing encryption tools annually and ensuring all team members use them. |
| Educate staff on phishing and scam awareness. |  |  |  | Conducting phishing simulations and regular awareness campaigns. |

1. Virtual Meetings protocol checklist

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cyber Safety Protocol Review Form | | | | |
| Rules | Full Compliance | Minor Non-Compliance | Major Non-Compliance | Suggested Improvements (If Necessary) |
| Implementing only approved video conferencing tools. |  |  |  | Regularly review the list of approved tools and ensure compliance. |
| Configuring meeting settings to require a password. |  |  |  | Try training staff on how to configure secure meeting settings effectively. |
| Limiting screen sharing to the host only unless necessary. |  |  |  | Providing guidelines on when and how to enable screen sharing. |
| Avoiding sharing sensitive information in public chats. |  |  |  | Educating participants on alternative secure methods for sharing data. |
| Recording meetings only when essential and permitted. |  |  |  | Utilizing a formal policy for recording approvals and storage. |
| Following a structured meeting agenda. |  |  |  | Distributing agendas at least 24 hours in advance to improve adherence. |

1. Select and evaluate two methods that could be utilised to share and distribute the knowledge gained from the compliance review with relevant personnel.
   * + 1. Internal Workshops or Training Sessions:

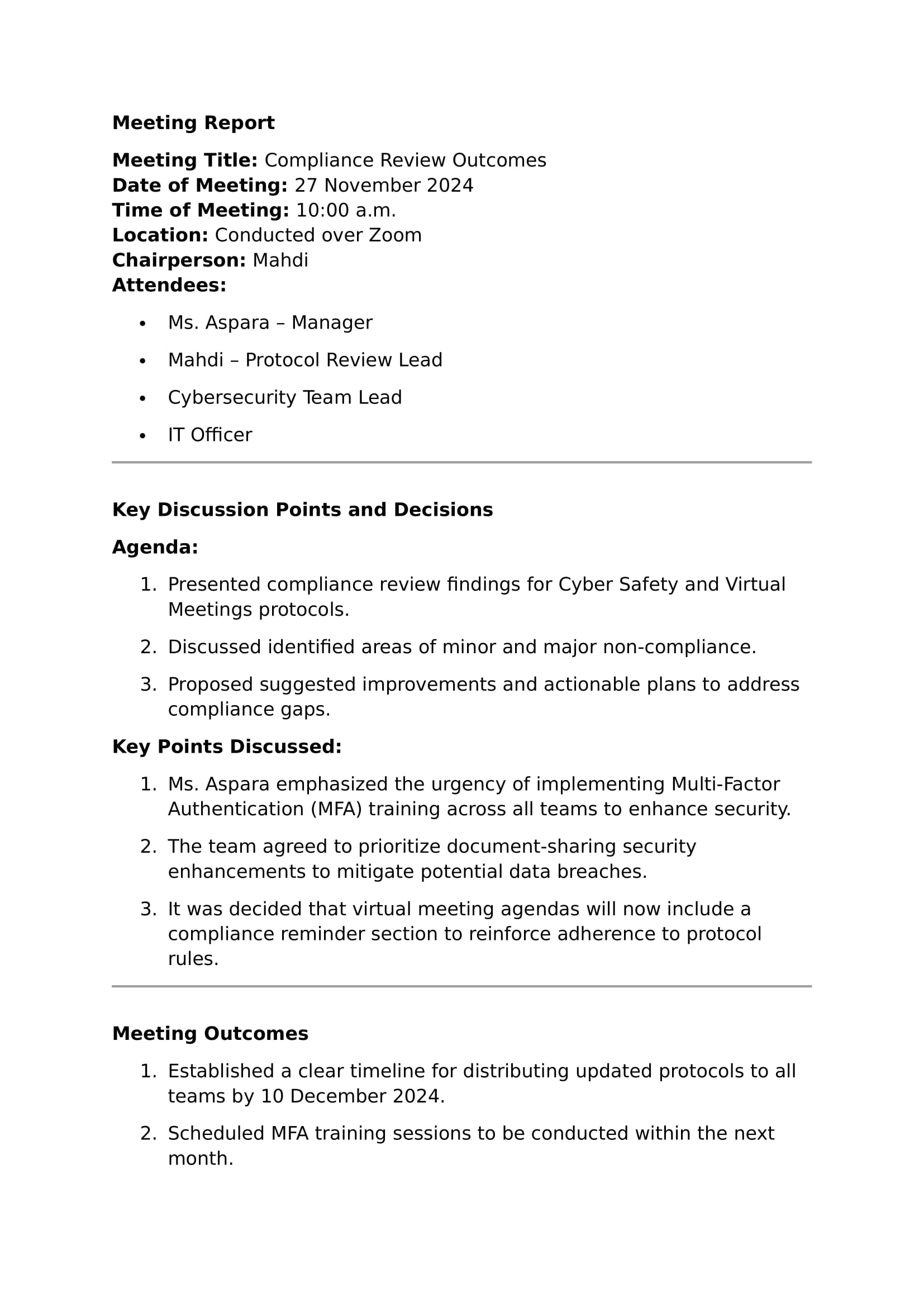
We are able to gather people in our organization and educate these employees on updated protocols and our findings to have better compliance. It encourages employees to open discussions and direct questions for better understanding.

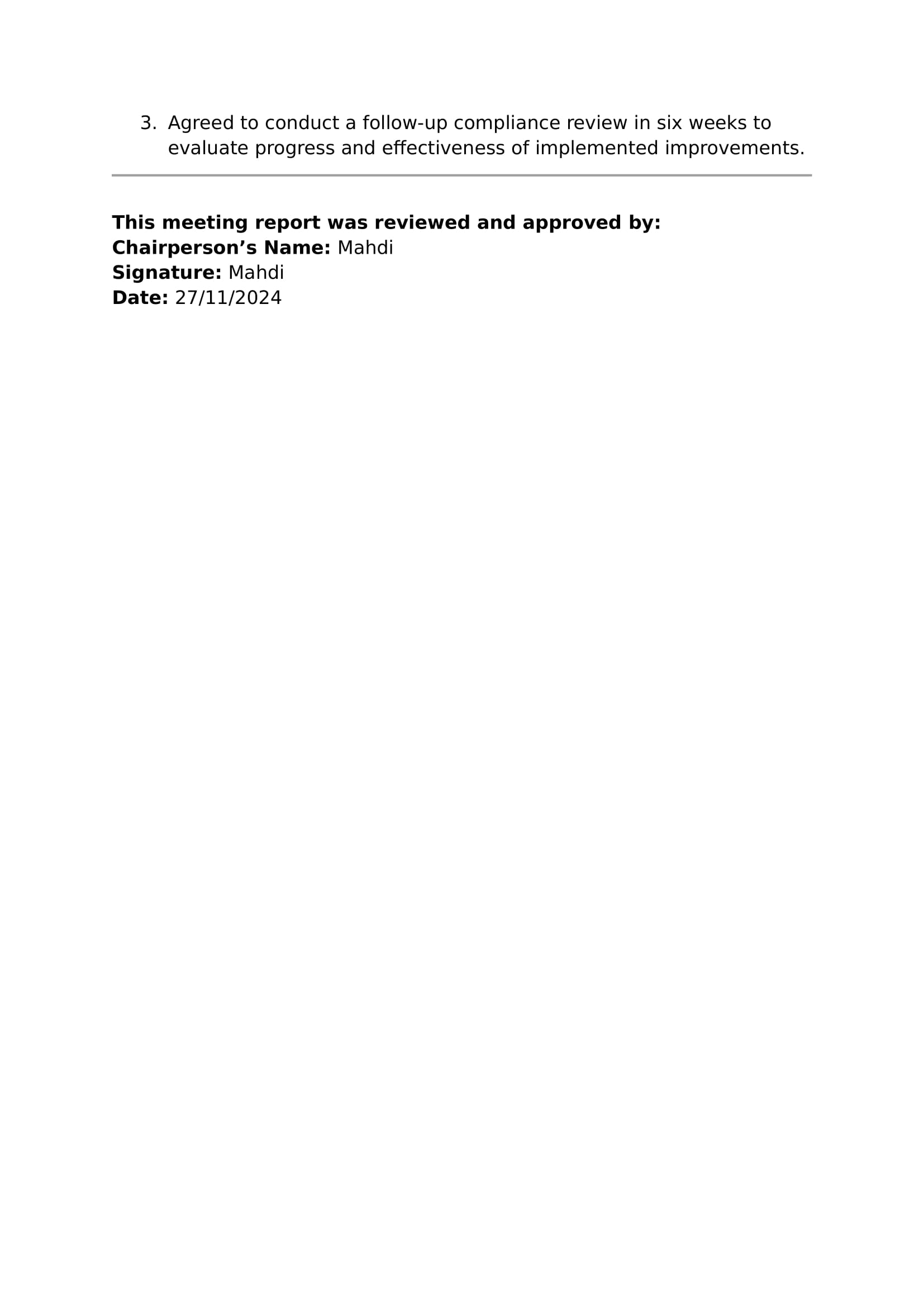
Digital Knowledge Repositories:

It is possible to upload findings and revised protocols into an internal system, like a cloud base sharing knowledge

It is going to be effective as it addresses demands and offers access to information as responses.

1. Arrange a meeting with the manager to discuss review outcomes. Document the meeting.



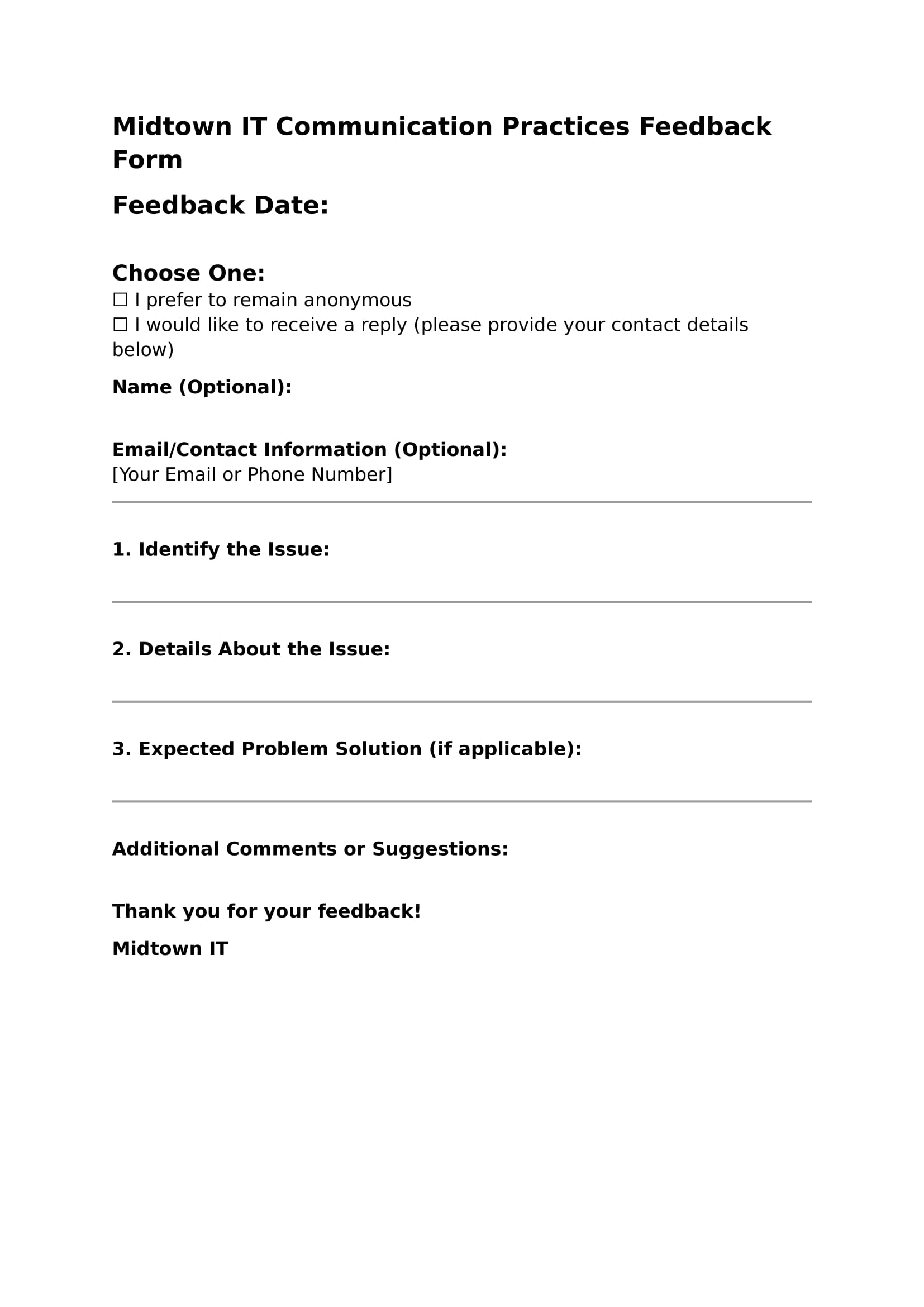


TASK 5 Collecting and replying to feedback

1. Create a feedback form that relevant personnel at Midtown IT can use to collect relevant information about the effectiveness of communication practices included in the two protocols written in TASK 1.

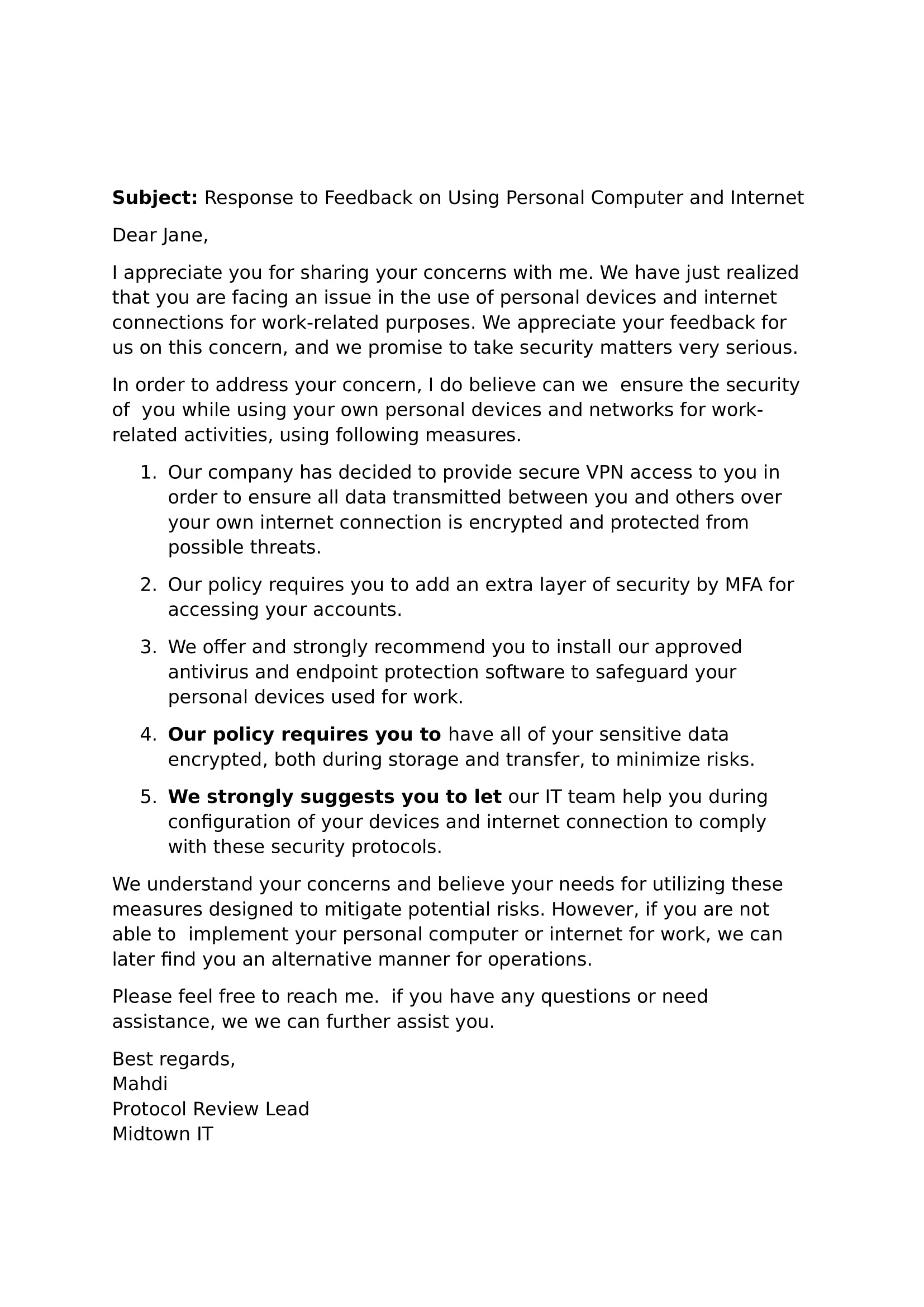
The feedback must include sections to:

1. Record feedback date
2. Allow a person to remain anonymous OR
3. Identify the person providing the feedback if they want to receive a reply
4. Identify the issue
5. Provide details about the issue
6. State the expected problem solution (if this applies)

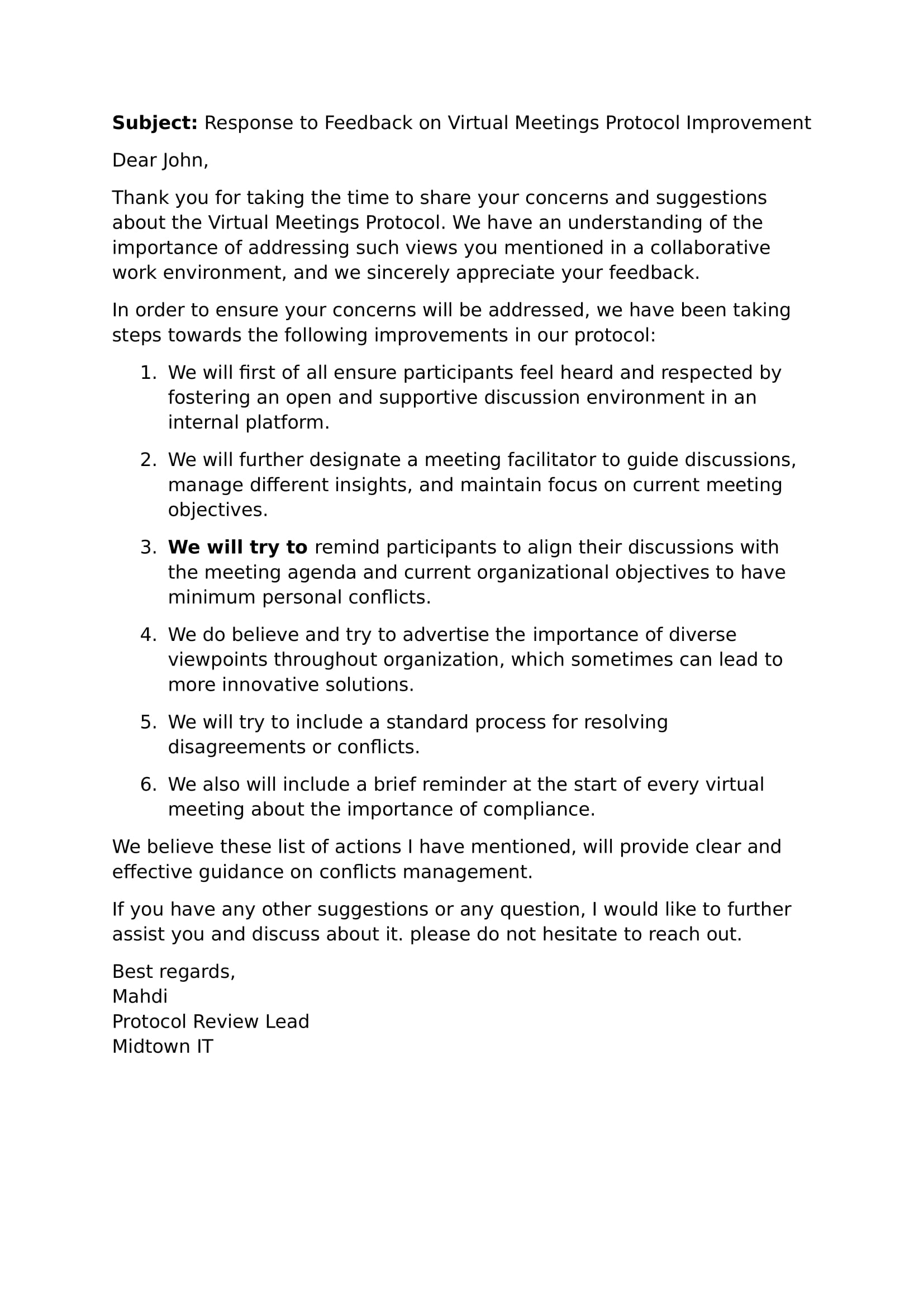


1. Jane, a consultant at Midtown IT, has provided feedback regarding her concerns about using her personal computer and internet connection for work-related purposes. Her main concern is security.

Write a reply to the feedback received. Hint – read the scenario provided.



1. John, a consultant at Midtown IT, has provided feedback. John wants to have the Virtual Meetings Protocol improved to include information about how to deal with conflicting views/perspectives in the collaborative work environment.

Write a reply to the feedback received. 

1. In addition to feedback forms, what other constructive feedback techniques could be used? List and briefly describe two (2) techniques.
   * + One-on-One Meetings: These can be done with private conversations between an employee and a manager or a team member. They will allow employees to express their possible concerns easily, provide feedback, and receive solutions by us.
     + 360-Degree Feedback: This method will enable us by gathering multiple feedback from diverse sources, such as peers, managers, or even sometimes clients. It can help us to provide comprehensive feedback of an employee’s performance, his communication, and collaboration practices.

**End of Assessment**