Assignment Guidance and Front Sheet

This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded to Moodle for students to fill in their ID and submit with their assessment.

Student ID or IDs for group work	Student fill in own ID and attach document for submission

Module Title & Code	WM244 - Information Security Management
Module Owner	Dr Olga Angelopoulou
Module Tutor	Dr Olga Angelopoulou
Module Marker	tbc
Assesment type	CW2: Information Security Framework of Policies
Date Set	10.10.22
Submission Date (excluding extensions)	14.03.23
Marks return date (excluding extensions)	20 working days from the date of the submission
Weighting of mark	50%

Assessment Detail	**Please refer to the Case Study and Useful Sources sections.** You are required to create a framework of policies in the format of one (1) page table that are UK Government compliant for the given organisation's IT infrastructure. The framework of policies you create must pass UK Government-based requirements. You should write an executive report of no more than two (2) pages that discusses 3 high-priority security controls for your organisation and any potentially optional elements of the framework. It is imperative that the executive report should have a professional look and be precise. After all it will be submitted to the firm's executive team as the result of your work. Also, it should include your justification behind your decisions. Any relevant notes of your work must be submitted as an appendix.

Additional details	There is no word count for this coursework as long as you adhere to the requirements of the submission:
	    a. One page table
	    b. Up to two pages report
	    c. Any additional work/ notes submitted in an appendix
	
	You should use a clear font in a font size that would be readabe when printed in A4 size paper. Recommended font sizes:
	    - Table: font size 9-11pt
	    - Report: font size 10-12pt

	If you utilise any appendices, then you should refer the reader to the relevant appendix within your report, otherwise the appendix will not be considered.
Module learning outcomes (numbered)	1 - Adopt a responsible attitude to the social, ethical, legal and regulatory consequences that flow from professional engagement in security management. 2 - Evaluate the overall coherence of an organisation's management of cyber security, recommending remediation where needed.
Learning outcomes assessed in this assessment (numbered)	1,2
Marking guidelines	You will be marked based on the following criteria: 1. *Completeness of the framework of policies* 2. *Consideration of issues/ Security controls* 3. *Justification of arguments* 4. *Presentation and design* **Please also refer to the University Marking Scale (attached below).**
Submission guidance	You must use the Harvard referencing system as per the University regulations. All submissions should be made in PDF format via Tabula https://tabula.warwick.ac.uk.
Academic Guidance	This coursework aims to guide you on writing a professional report in a non-verbose manner. Additional guidelines if necessary will also be provided in a class briefing session.
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that "earliest opportunity" means in terms of timing and other arrangements is different depending on Programme (i.e. Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised to consult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.

Case Study

You work for a high-tech company with approximately 400 employees. Your firm recently won a large UK Government contract, which will add 30% to the revenue of your organization. It is a high-priority, high-visibility project. You will be allowed to make your own budget, project timeline, and take decisions.

Currently, your organisation does not have any UK Government contracts and thus has no UK Government-compliant security policies or controls in place.

You have been assigned as the group leader to develop the appropriate security policies required to meet UK Government standards for delivery of technology services. In order to achieve this, you must develop a framework of UK Government-approved policies and standards for your IT infrastructure (see below).

In order to complete the task, you should work on and consider the following:

- Any compliance laws required for UK Government contracts.
- Any controls relevant to the IT infrastructure.
- Any required standards for all your devices, based on the IT infrastructure.
- A deployment plan for implementation of these polices, standards, and controls.
- All applicable UK Government frameworks.

The firm's computing environment includes the following:

- 12 servers running Microsoft Server 2019, providing the following:

- Active Directory (AD)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Enterprise Resource Planning (ERP) application (Oracle)
- A Research and Development (R&D) Engineering network segment for testing, separate from the production environment
- Microsoft Exchange Server for e-mail
- Symantec e-mail filter
- Symantec Advanced Secure Gateway for Internet use

- Two Linux servers running Apache Server to host your website

- 460 PCs/laptops running Microsoft Windows 10 Enterprise, Microsoft Office 365, Microsoft OneDrive for Business, Microsoft Visio, Microsoft Project, and Adobe Reader.

Useful Sources

The following sources will allow you to familiarise with essential material you should study before you work on this assignment:

- Government technology standards and guidance
- The National Cyber Security Centre
- NCSC CAF Framework
- Security policy framework: protecting government assets
- Security policy framework: legal guidance
- Security Requirements for Contractors
- Cyber Essentials Scheme

Marking scale

Class	Scale	Mark	Descriptor
First	Excellent 1st	100	Work of original and exceptional quality which in the examiners' judgement merits special recognition by the award of the highest possible mark.
		94	Exceptional work of the highest quality, demonstrating excellent knowledge and understanding, analysis, organisation, accuracy, relevance, presentation and appropriate skills. At final-year level: work may achieve or be close to publishable standard.
	High 1st	88	Very high quality work demonstrating excellent knowledge and understanding, analysis, organisation, accuracy, relevance, presentation and appropriate skills. Work which may extend existing debates or interpretations.
	Upper Mid 1st	82	
	Lower Mid 1st	78	
	Low 1st	74	
Upper Second (2.1)	High 2.1	68	High quality work demonstrating good knowledge and understanding, analysis, organisation, accuracy, relevance, presentation and appropriate skills.
	Mid 2.1	65	
	Low 2.1	62	
Lower Second	High 2.2	58	Competent work, demonstrating reasonable knowledge and understanding, some analysis, organisation, accuracy, relevance, presentation and appropriate skills.
	Mid 2.2	55	
	Low 2.2	52	
Third	High 3rd	48	Work of limited quality, demonstrating some relevant knowledge and understanding.
	Mid 3rd	45	
	Low 3rd	42	
Fail	High Fail (sub Honours)	38	Work does not meet standards required for the appropriate stage of an Honours degree. Evidence of study and demonstrates some knowledge and some basic understanding of relevant concepts and techniques, but subject to significant omissions and errors.
	Fail	32	Work is significantly below the standard required for the appropriate stage of an Honours degree. Some evidence of study and some knowledge and evidence of understanding but subject to very serious omissions and errors.
		25	Poor quality work well below the standards required for the appropriate stage of an Honours degree.
	Low Fail	12	
Zero	Zero	0	Work of no merit OR Absent, work not submitted, penalty in some misconduct cases