|  |  |  |  |
| --- | --- | --- | --- |
| **Assignment Front Sheet** | | | |
| Learner name | Assessor name | | |
|  | Philomena Dillon | | |
| Date Issued | Completion date | | Submitted on |
| 5th February | 18th Mach 2013 | |  |
| Qualification | | Unit number and title | |
| BTEC National Extended Diploma in IT | | 07 – Organisational Systems Security | |
| Assignment title | Assignment 1 – Understanding system security! | | |
| In this assignment you will have opportunities to provide evidence against the criteria shown in the next boxes.  Indicate the page numbers where the evidence can be found  PLEASE NOTE THAT OTHER CRITERIA FOR THIS UNIT WILL BE ADDRESSED IN FURTHER ASSIGNMENT(S). | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Criteria reference | To achieve the criteria the evidence must show that the student is able to: | Task no. | Evidence | Page |
| P2 | Explain the impact of different types of threats on an organisation. | 1 | Report |  |
| P3 | Describe how physical security measures can help keep systems secure. | 2 | Report |  |
| P1 | describe how software and network security can keep systems and data secure | 3 | Report |  |
| M1 | discuss information security | 4 | Report |  |
| M2 | Explain the operation and use of an encryption technique in ensuring security of transmitted information. | 5 | Report |  |

|  |
| --- |
| Learner declaration |
| I certify that the work submitted or this assignment is my own and research sources are fully acknowledged.  Learner signature: Date: |

|  |  |
| --- | --- |
| **Assignment brief** | |
| Qualification | BTEC Level 3 National Extended Diploma in I.T. |
| Unit number and title | 07 – Organisational Systems Security |
| Start date | 5th February 2013 |
| Deadline | 12th March 2013 |
| Assessor name | Philomena Dillon |
|  | |
| Assignment title | Assignment 1 – Understanding system security! |
| The purpose of this assignment is to: Help students to understand the impact of potential threats to IT systems | |
| **Basic Scenario:** Produce a report describing how you would keep computer systems secure and the reasoning behind the security.  **Note**  You will need to research the subject using a variety of sources i.e. text books, eBooks, journals, help files and the Internet. Any direct quotes must be referenced using the Harvard Referencing System.  You will need to have proper headings and sub headings, a contents page, page numbers in the bottom right-hand footer in the format page x of y and your full name in the top right-hand header.  The report needs to have a front cover with the unit number, unit description, assignment number, assignment description and your name. | |
| **Task 1**  Learners must research and develop a list of physical security measures to help prevent attacks of any kind. It would be useful if you **described** the measure and what you consider to be the effectiveness of each measure provided.  A combination of methods would produce a much more secure system so by all means put into your report any combinations you think would complement each other.  **P2** | |
| **Task 2**  Learners must **describe** software and network security measures that they would recommend to keep a commercial computer system secure.  A combination of methods would produce a much more secure system so by all means put into your report any combinations you think would complement each other. **P3** | |
| **Task 3**  Learners must **explain** the impact of at least 4 different types of threat on an organisation. You must suggest different issues arising from theft or damage to hardware and the theft or damage to data within a given organisation. In this case South Nottingham College.  **P1** | |
| **Task 4**  Learners must **discuss** information security. Using your research from Task 3 you should develop strategies that would help to reduce the REAL threats that a college faces each day from both physical and software threats.  **M1** | |
| **Task 5**  Learners must **explain** the operation and use of encryption using South Nottingham College as a base company. Discuss areas of the college where encryption is paramount and areas where it might be useful to encrypt data to ensure security when transmitting the data to other secure computer systems.  **M2** | |
| **Help page for assignment**  **Understand the impact of potential threats to IT systems**  *Potential threats:* malicious damage; threats related to e-commerce; counterfeit goods; technical failures;  other e.g. human error, theft of equipment  *Malicious damage*: internal; external; access causing damage e.g. viruses; access without damage; specific  examples e.g. phishing, identity theft, piggybacking, hacking  *Threats related to e-commerce*: website defacement; control of access to data via third party suppliers;  other e.g. denial of service attacks  *Counterfeit goods*: products at risk e.g. software, DVDs, games, music; distribution mechanisms e.g. boot  sales, peer-to-peer networks  *Organisational impact*: loss of service; loss of business or income e.g. through loss of customer records;  increased costs; poor image  *Information security*: confidentiality; data integrity; data completeness; access to data  **Know how an organisation can keep systems and data secure**  *Physical security*: locks; visitors passes; sign in/out systems; biometrics e.g. retinal scans, fingerprint, voice  recognition; others e.g. guards, cable shielding  *Software and network security*: encryption techniques e.g. public and private key; call back; handshaking;  diskless networks; use of backups; audit logs; firewall configuration; virus checking software; use of virtual  private networks (VPN); intruder detection systems; passwords; levels of access to data; software updating;  disaster recovery e.g. backup systems, whole system replacement, tiers of recovery  **Understand the organisational issues affecting the security of IT systems**  *Security policies and guidelines*: disaster recovery policies; updating of security procedures; scheduling  of security audits; codes of conduct e.g. email usage policy, internet usage policy, software acquisition,  installation policy; surveillance policies; risk management; budget setting  *Employment contracts and security*: hiring policies; separation of duties; ensuring compliance including  disciplinary procedures; training and communicating with staff as to their responsibilities  *Laws*: legislation e.g. Computer Misuse Act 1990; Copyright, Designs and Patents Act 1988; privacy and  compensation requirements of Data Protection Act 1984, 1998, 2000  *Copyrights*: open source; freeware; shareware; commercial software  *Ethical decision making*: e.g. freedom of information versus personal privacy (electoral roll, phone book and  street maps put together); permission e.g. to use photographs or videos, CCTV footage  *Professional bodies*: organisations e.g. Business Software Alliance (BSA), Federation Against Software Theft  (FAST), British Computing Society (BCS), Association of Computing Machinery (ACM)  **Indicative reading for learners**  **Textbooks**  Beekman G and Quinn M J – *Computer Confluence Complete: and Student CD – 1st international edition*  (Pearson Education, 2005) ISBN-10 1405835796, ISBN-13 978-1405835794  Heathcote P – *A Level ICT – revised edition* (Payne Gallway, 2004) ISBN-10 0953249085, ISBN-13 978-0953249084  **Websites**  www.acm.org Association of Computing Machinery  www.bcs.org British Computing Society  www.bsa.org.uk Business Software Alliance  www.fast.org.uk Federation Against Software Theft  www.ico.gov.uk Information Commissioner’s Office | |

|  |  |  |  |
| --- | --- | --- | --- |
| This brief has been verified as being fit for purpose | | | |
| Assessor | Philomena Dillon | | |
| Signature |  | Date |  |
| Internal verifier |  | | |
| Signature |  | Date |  |