Computers

VOCABULARY PRACTICE

ADVANCED | C1

Name: _____ **Date:** _____

1 Match each advanced digital-governance concept with its meaning.

1 algorithmic bias	____	a record of where data originated and how it changed
2 model opacity	____	b input deliberately altered to mislead a computational model
3 data provenance	____	c inability to understand how a model reached an output
4 interoperability	____	d privacy method adding controlled statistical noise
5 vendor lock-in	____	e systematic unfairness produced or reinforced by an algorithm
6 attack surface	____	f system design that verifies every access request
7 zero-trust architecture	____	g training across separate devices without centralising raw data
8 adversarial example	____	h difficulty moving away from a supplier's proprietary system
9 differential privacy	____	i all points through which a system might be attacked
10 federated learning	____	j ability of different systems to exchange and use information

2 Complete the digital-governance collocations.

audit | explainability | framework | lock-in | provenance | surface | threat | trust

1 establish data _____

2 reduce the attack _____

3 conduct an algorithmic _____

4 improve model _____

5 define an accountability _____

6 adopt zero _____

7 avoid vendor _____

8 perform _____ modelling

3 Choose the concept that best captures the distinction.

1 Historic patterns create unequal automated outcomes: *algorithmic bias / opacity*.

2 Reviewers cannot reconstruct a dataset's origins: *data provenance / interoperability*.

3 A supplier's format makes migration costly: *vendor lock-in / attack surface*.

4 Each request is verified regardless of location: *zero trust / federated learning*.

5 Noise protects individuals in published statistics: *differential privacy / encryption*.

6 Hospitals train a model without pooling records: *federated learning / provenance*.

Computers

VOCABULARY PRACTICE

ADVANCED | C1

4 Complete the system-governance review with terms from the box.

algorithmic bias | attack surface | data provenance | differential privacy | federated learning | interoperability | model opacity | vendor lock-in | zero-trust architecture

The review documents **1** _____ and tests for **2** _____ across demographic groups. Because **3** _____ limits meaningful explanation, high-impact outputs require human review. Open standards improve **4** _____ and reduce **5** _____. A **6** _____ limits implicit trust, while service consolidation reduces the **7** _____. The research partnership uses **8** _____ to keep raw records local and **9** _____ when releasing aggregate statistics.

5 Read the text and answer the questions concisely.

Governing an automated allocation system

A public agency used a predictive model to prioritise inspections. Overall accuracy appeared high, but errors were concentrated in neighbourhoods poorly represented in the training data. The agency paused automatic referrals, published subgroup performance measures and commissioned an independent audit. It retained the model only as decision support, established an appeal route and scheduled monitoring for distribution shift. Procurement terms also required exportable data and documented interfaces so the agency could change suppliers.

1 What did the model prioritise? _____

2 What did overall accuracy conceal? _____

3 Name two immediate safeguards. _____

4 What role did the model retain? _____

5 Why was distribution shift monitored? _____

6 How did procurement reduce dependence on one supplier? _____

6 Paraphrase using the expression in capitals.

1 The model's reasoning cannot be interpreted clearly. **OPACITY** ___

2 The systems can exchange and use data. **INTEROPERABLE** _____

3 Every request is verified before access. **ZERO-TRUST** _____

4 The supplier is difficult and costly to replace. **LOCK-IN** _____

OVER TO YOU

Write a **160-190 word** governance proposal for a high-impact computer system. Address data, bias, explainability, security, human oversight, appeals, monitoring and supplier dependence.

[ ] Use at least ten target terms or collocations. [ ] Link each risk to a safeguard. [ ] Define accountability and review.

ANSWER KEY

1 Advanced digital-governance concepts

1 **e** 2 **c** 3 **a** 4 **j** 5 **h** 6 **i** 7 **f** 8 **b** 9 **d** 10 **g**

2 Digital-governance collocations

1 **provenance** 2 **surface** 3 **audit** 4 **explainability** 5 **framework** 6 **trust** 7 **lock-in** 8 **threat**

3 Conceptual distinctions

1 **algorithmic bias** 2 **data provenance** 3 **vendor lock-in** 4 **zero trust**
5 **differential privacy** 6 **federated learning**

4 System-governance review

1 **data provenance** 2 **algorithmic bias** 3 **model opacity** 4 **interoperability** 5 **vendor lock-in**
6 **zero-trust architecture** 7 **attack surface** 8 **federated learning** 9 **differential privacy**

5 Reading - suggested answers

1 Inspections. 2 Errors concentrated in underrepresented neighbourhoods. 3 Pausing referrals, subgroup measures or an audit.
4 Decision support only. 5 To detect changing data patterns. 6 It required exportable data and documented interfaces.

6 Paraphrasing - possible answers

1 The model suffers from **opacity**. 2 The systems are **interoperable**. 3 It uses a **zero-trust architecture**. 4 The agency faces vendor **lock-in**.

Over to you: Answers will vary. Check conceptual precision, traceable safeguards, oversight and contestability.