Exercises

1	2	3	4	5	6	7

1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6
7	7	7	7	7	7	7
8	8	8	8	8	8	8
9	9	9	9	9	9	9
0	0	0	0	0	0	0

Surname, First name

Principles of data protection (2IMS25)
Resit

Particular Ans on paper exam instructions

- Write in a black or blue pen.
- You answer open-ended questions by using the text box. Provide your answers on the papers inside the answer box underneath a question. **If you need more space for your answers, use the extra space at the end of the exam, and clearly indicate there which question you continue answering. In the text box of the particular question, clearly state that you proceed with your answer on a different page.**
- Hand in all pages. Do not remove the staple. If you remove it anyhow, check that you hand in all pages.

Dear student,
You're about to take an exam. Write down your name and your student ID at the appropriate places above. Make sure that you enter your student ID by fully coloring the appropriate boxes. On the examination attendance card, you fill in the PDF number. You can find the correct number on the top of the first page of your exam (e.g. 1234.pdf).

Please read the following information carefully:
Date exam: 2/2/2022
Start time 18.00
End time: 21.00 (+30 minutes for time extension students)

Number of questions: 6
Maximum number of points/distribution of points over questions: 10
Method of determining the final grade: Final exam
Answering style: formulation, order, foundation of arguments, multiple choice:

Permitted examination aids: None

Important:

- You are only permitted to visit the toilets under supervision
- Examination scripts (fully completed examination paper, stating name, student number, etc.) must always be handed in
- The house rules must be observed during the examination

- The instructions of subject experts and invigilators must be followed
- Keep your work place as clean as possible: put pencil case and breadbox away, limit snacks and drinks
- You are not permitted to share examination aids or lend them to each other
- Do not communicate with any other person by any means

During written examinations, the following actions will in any case be deemed to constitute fraud or attempted fraud:

- using another person's proof of identity/campus card (student identity card)
- having a mobile telephone or any other type of media-carrying device on your desk or in your clothes
- using, or attempting to use, unauthorized resources and aids, such as the internet, a mobile telephone, smartwatch, smart glasses etc.
- having any paper at hand other than that provided by TU/e, unless stated otherwise
- copying (in any form)
- visiting the toilet (or going outside) without permission or supervision

You can start the exam now, good luck!

DAC

Recall the HRU model.

1.5p **1** a) Compute the access matrix that results from the following initial state

	File 1	File 2	Process 1
Alice			own
Bob	own	*read	
Charlie	write	own	
David			

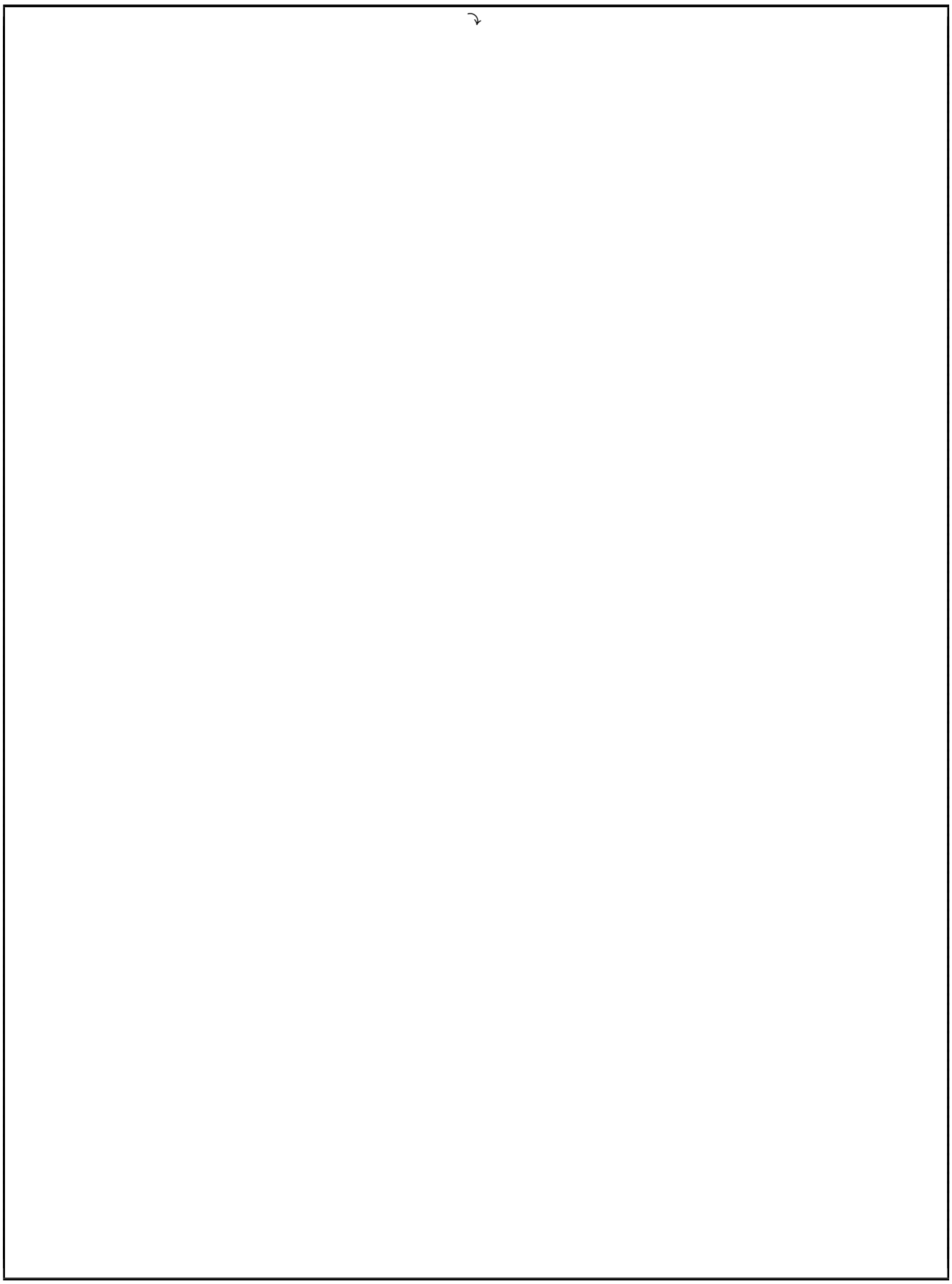
by executing the sequence of commands α defined as follows:

1 $CONFER_{*exec}(Alice, Charlie, Process1)$
2 $TRANSFER_{exec}(Charlie, Bob, Process1)$
3 $CONFER_{*read}(Bob, Alice, File2)$
4 $CREATE(Alice, File1)$
5 $CONFER_{*write}(Alice, Alice, File1)$
6 $CONFER_{*write}(Alice, Bob, File1)$
7 $REVOKE_{exec}(Charlie, Bob, Process1)$
8 $TRANSFER_{read}(Alice, David, File2)$
9 $CREATE(Bob, Process2)$
10 $TRANSFER_{exec}(Bob, Alice, Process2)$
11 $TRANSFER_{exec}(Bob, Charlie, Process2)$
12 $REVOKE_{exec}(Charlie, Charlie, Process1)$
13 $TRANSFER_{exec}(Charlie, David, Process1)$
14 $REVOKE_{exec}(Alice, David, Process1)$
15 $REVOKE_{read}(Charlie, David, File2)$
16 $TRANSFER_{write}(Alice, David, File1)$
17 $TRANSFER_{exec}(Alice, David, Process2)$
18 $REVOKE_{exec}(Bob, David, Process2)$
19 $REVOKE_{write}(Bob, David, File1)$
20 $REVOKE_{exec}(Bob, Alice, Process2)$

Hints:

- Command $CONFER_{*read}$ is equal to $CONFER_{read}$ but grants $*read$ instead of $read$. Similar principle applies to $CONFER_{*exec}$ and $CONFER_{*write}$.
- Command $REVOKE_{read}$ removes both $read$ and $*read$. Similar principle applies to $REVOKE_{exec}$ and $REVOKE_{write}$.

b) Does α leak access privileges? (Consider only David to be untrusted) Justify your answer.



MAC

1.5p **2** The Biba model assumes the strong tranquility property. Explain (a) what the strong tranquility property means, (b) how the integrity policy enforced by the Biba model has been relaxed while preserving the information flow, and (c) give an example in which the "relaxed" Biba model(s) can be applied.

RT

1p **3a** Consider the following RT_0 policy.

$A.t \leftarrow A.t.s$
$A.t \leftarrow K.t \cap L.t$

$K.t \leftarrow A$
$K.t \leftarrow D$
$K.t \leftarrow E$

$L.t \leftarrow D$
$L.t \leftarrow E$

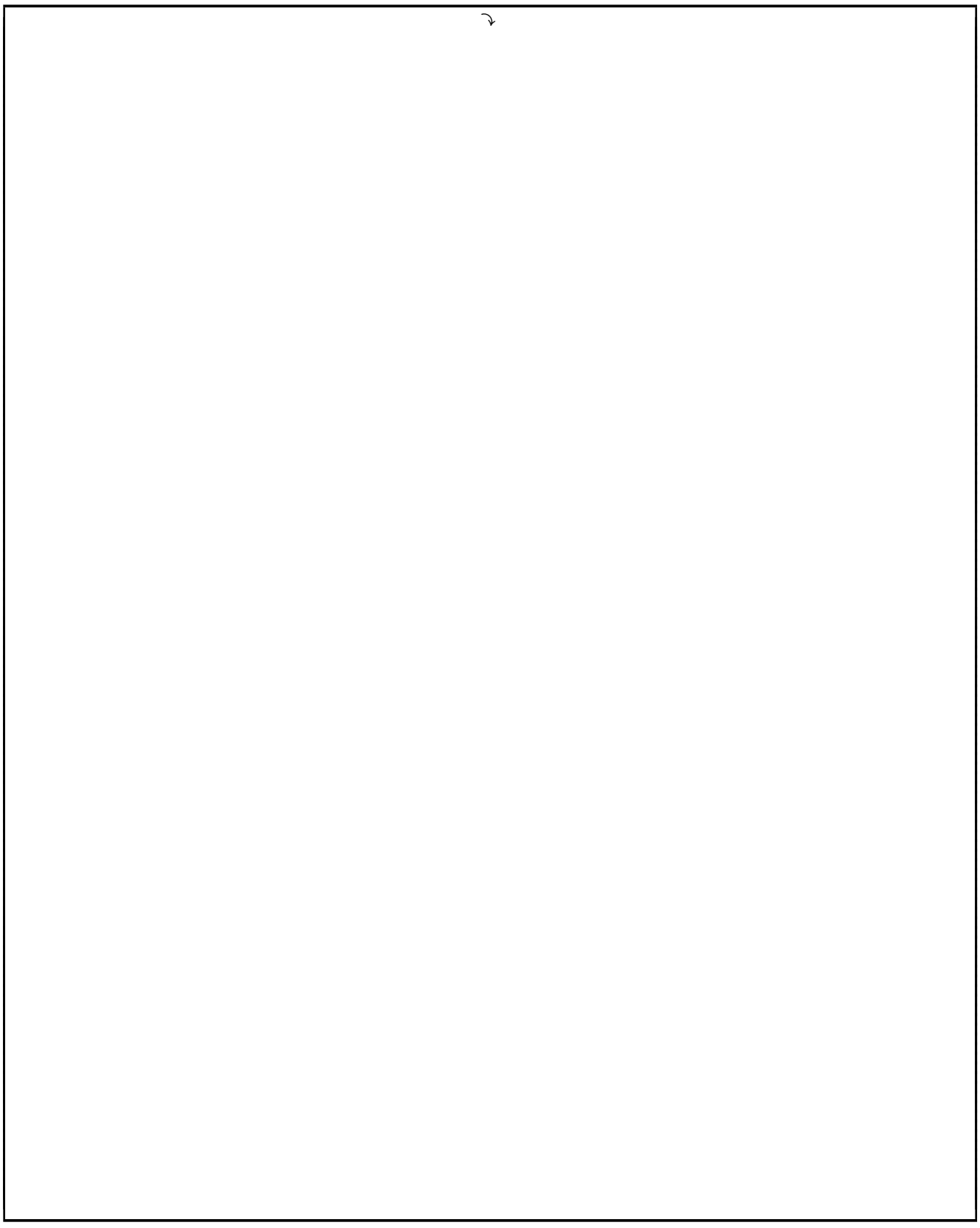
$D.s \leftarrow L$
$D.s \leftarrow M$
$D.s \leftarrow H$

$H.t \leftarrow W$

$H.s \leftarrow Z$

$Z.s \leftarrow W$

1. Find all principals populating $A.t$ (which means, compute $[[A.t]]$).
2. Write down the graph generated by the top-down algorithm when computing the semantics of $A.t$. (the top-down algorithm is also known as the "backward algorithm").



1p **3b** Consider a University that we conventionally call the TUe. Assume it has only three faculties: EL, IE, and CS. Each faculty uses RT to maintain the list of lecturers, the list of students and the list of "operators" (non-academic staff). The TUe has a library. Consider the following policy statements.

- All students of any faculty of the TUe have access to the library of the TUe.
- All operators working for all three faculties are eligible for an end-of-year bonus
- Alice is a student of EL
- Tom is an operator of CS
- Luca is a lecturer of IE

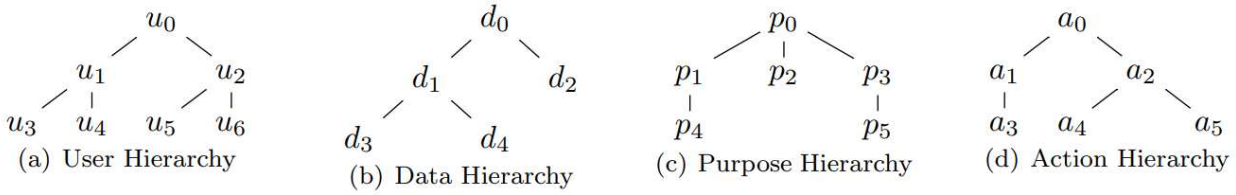
Write down an RT policy to model the above statements. Try to make use of a linked role for the first statement.

Purpose-based Access Control

1.5p **4** In Purpose-based Access Control, the access decision making process comprises two steps. Explain (a) what these steps are, (b) what their goal is, and (c) why they are needed.

EPAL

Let $Voc = (UH, DH, PH, AH, OM)$ be a vocabulary where the user hierarchy UH, data hierarchy DH, purpose hierarchy PH and action hierarchy AH are defined in the figure below, and $OM = (O, \rightarrow)$ is the obligation model with $O = \{o1, o2, o3, o4, o5, o6\}$ and $\rightarrow = \{o2 \rightarrow o3, o2 \rightarrow o5, o6 \rightarrow o2\}$.



(a) User Hierarchy (b) Data Hierarchy (c) Purpose Hierarchy (d) Action Hierarchy

Consider the following EPAL policies defined over Voc:

$pol_1 =$
$\langle (u_2, d_3, p_0, a_4)(+, true, \{o_1\}) \rangle$
$\langle (u_1, d_3, p_2, a_0)(\circ, true, \{o_2\}) \rangle$
$\langle (u_4, d_0, p_4, a_2)(+, true, \{o_3, o_4\}) \rangle$
$\langle (u_6, d_2, p_5, a_3)(-, true, \{o_4\}) \rangle$
$\langle (u_1, d_0, p_1, a_0)(\circ, true, \{o_5\}) \rangle$
Default ruling: $-$
Default obligations: $\{o_6\}$

$pol_2 =$
$\langle (u_2, d_3, p_0, a_4)(+, true, \{o_1\}) \rangle$
$\langle (u_1, d_3, p_2, a_0)(\circ, true, \{o_2\}) \rangle$
$\langle (u_4, d_0, p_4, a_2)(+, true, \{o_4, o_6\}) \rangle$
$\langle (u_6, d_2, p_5, a_3)(-, true, \{o_4\}) \rangle$
$\langle (u_1, d_0, p_1, a_0)(\circ, true, \{o_5\}) \rangle$
$\langle (u_0, d_0, p_0, a_0)(-, true, \{o_5\}) \rangle$
Default ruling: $-$
Default obligations: $\{o_6\}$

$pol_3 =$
$\langle (u_2, d_3, p_0, a_4)(+, true, \{o_1\}) \rangle \langle (u_1, d_3, p_2, a_0)(\circ, true, \{o_2\}) \rangle$
$\langle (u_4, d_0, p_4, a_2)(+, true, \{o_3, o_4\}) \rangle$
$\langle (u_6, d_2, p_5, a_3)(-, true, \{o_4\}) \rangle$
$\langle (u_6, d_2, p_3, a_1)(+, true, \{o_4\}) \rangle$
$\langle (u_1, d_0, p_1, a_0)(\circ, true, o_6) \rangle$
Default ruling: $-$
Default obligations: $\{o_6\}$

1.5p **5** Determine whether:

1. pol_2 is a refinement of pol_1,
2. pol_3 is a refinement of pol_1.

Justify your answer.

XACML

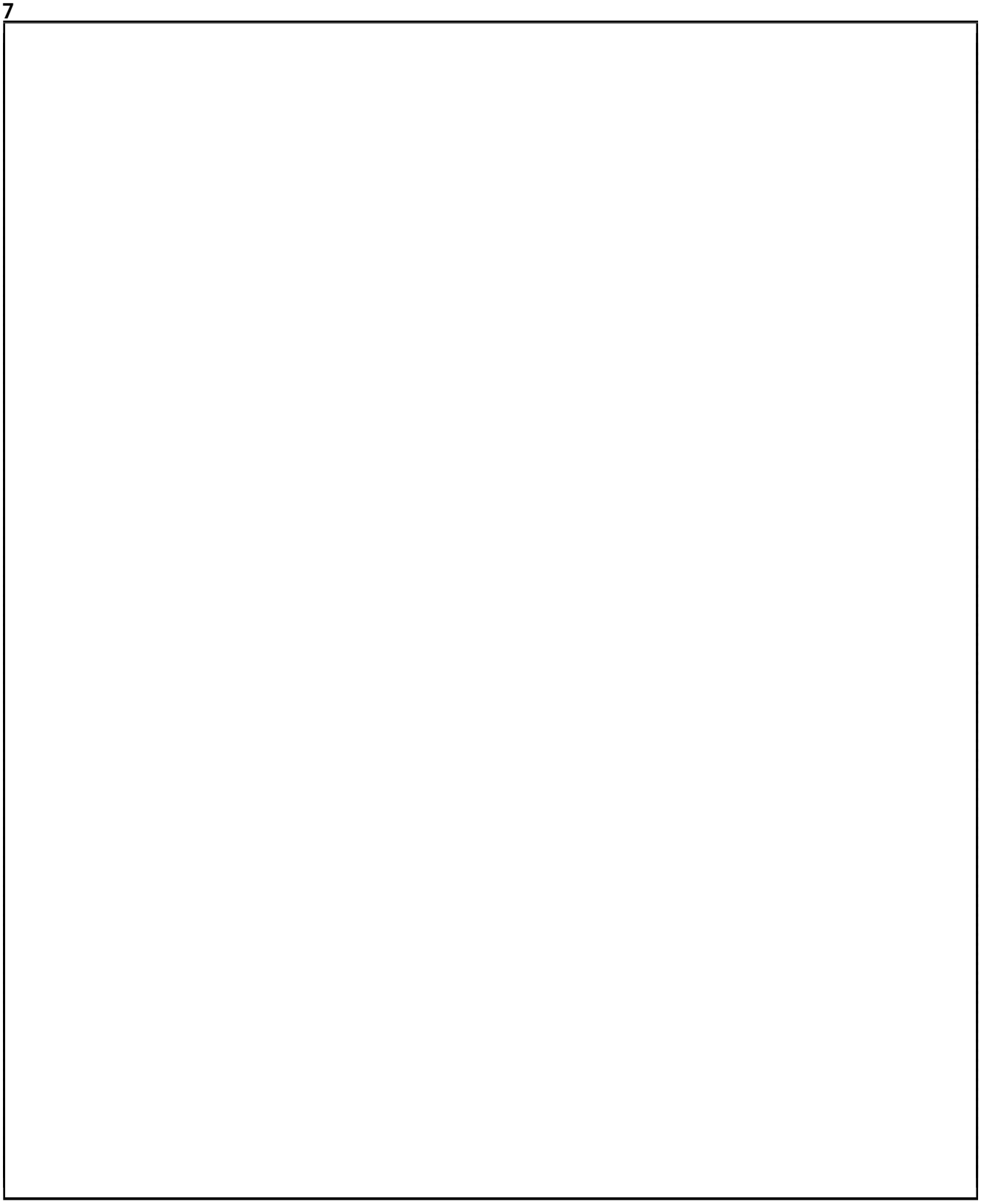
2p **6** Given the XACML policy and access request in attachment, determine the access response. Justify your answer.

Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Recall that rule evaluation and some combining algorithms are defined over the extended Indeterminate set ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). Decisions in the extended Indeterminate set indicate the potential decision(s) (Permit or Deny) that would have returned if an error have not occurred in the evaluation.

Extra space

7



This page is left blank intentionally

Access Request

```
  <Request>
   <Attributes
         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Alice
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                accountant
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                FinacialRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                read
            </AttributeValue>
         </Attribute>
    </Attributes>
  </Request>
```

```
<PolicySet PolicySetId="PS"
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-overrides">
  <Target>
       <AnyOf>
          <AllOf>
           <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 FinacialRecord
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
          </AllOf>
        </AnyOf>
  </Target>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit">
    <Target />
    <Rule Effect="Permit" RuleId="R1">
      <Target>
       <AnyOf>
         <AllOf>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  clerk
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                  15:00
               </AttributeValue>
               <AttributeDesignator MustBePresent="true"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                   DataType="http://www.w3.org/2001/XMLSchema#time"/>
           </Match>
         </AllOf>
         <AllOf>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  accountant
```

```
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
               15:00
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
               DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R2">
  <Target>
   <AnyOf>
     <AllOf>
       <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               accountant
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </Match>
       <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               write
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
               AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </Match>
     </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R3">
  <Target>
   <AnyOf>
     <AllOf>
       <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
```

```
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
               15:00
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
               DataType="http://www.w3.org/2001/XMLSchema#time"/>
         </Match>
         <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               accountant
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
       </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
   RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-overrides">
  <Target />
  <Rule Effect="Permit" RuleId="R4">
    <Target>
      <AnyOf>
       <AllOf>
         <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               accountant
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
         <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               manager
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
```

```
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Rule Effect="Deny" RuleId="R5">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 accountant
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 15:00
              </AttributeValue>
              <AttributeDesignator MustBePresent="true"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="03" />
    <Obligation FulfillOn="Deny" ObligationId="04" />
  </Obligations>
</Policy>
<Obligations>
  <Obligation FulfillOn="Permit" ObligationId="05" />
  <Obligation FulfillOn="Deny" ObligationId="06" />
</Obligations>
</PolicySet>
```