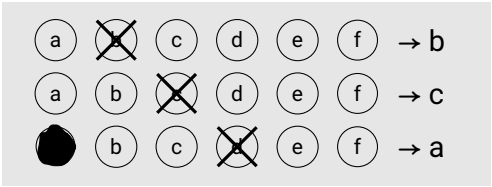
Exercises

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)
Final exam



Fill in your answer(s) to the multiple-choice questions as shown above (circles = one correct answer).

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: 09/11/2022
Start time 13.30
End time: 16.30 (+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

First-year bachelor students: The final grade for this exam will be announced no later than fifteen working days after the date of this exam, unless this exam takes place in Q4 or the interim period. For Q4 final exams, grades will be announced within five working days after the end of the Q4 final test period. For interim period final exams, grades will be announced no later than five working days before September 1.
All other students: Generally, the final grade for this exam will be announced no later than fifteen working days after the date of this examination. Specifically for bachelor exams administered in the interim period, exam grades will be announced no later than five working days before September 1.

You can start the exam now, good luck!

RBAC

1.5p **1** RBAC has been proposed to facilitate the specification and management of permissions compared to earlier access control models. Nonetheless, RBAC is not scalable.

1. Explain the limitations of RBAC with respect to scalability and conceive a situation in which these limitations arise.
2. Explain how these limitations can be addressed.

RT

1p **2a** Consider the following RT_0 policy.

$A.t \leftarrow A.t.s$
$A.t \leftarrow B.t$

$B.t \leftarrow J$
$B.t \leftarrow K$

$J.s \leftarrow J.t.s$

$B.r \leftarrow A$
$B.r \leftarrow B$

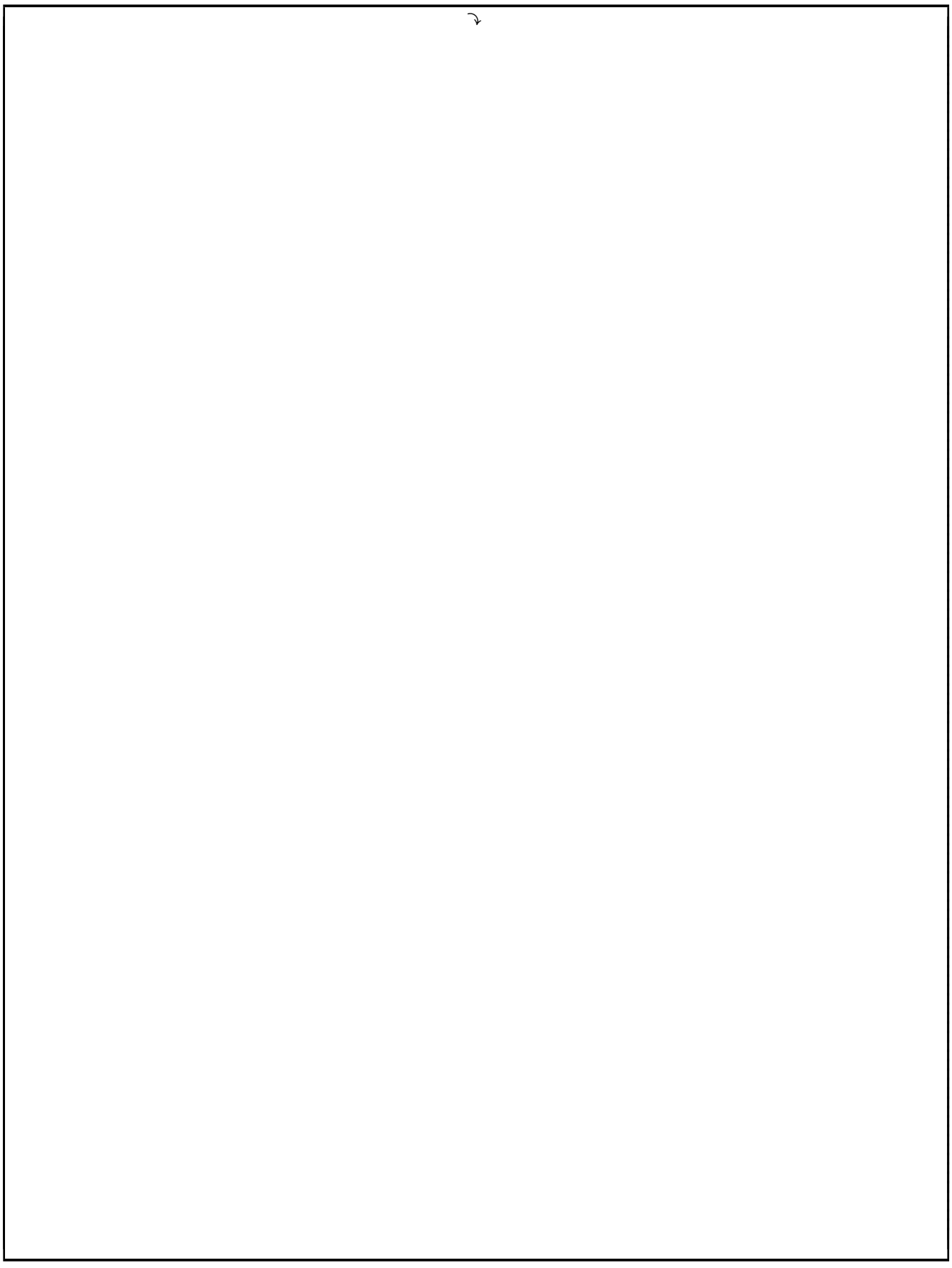
$K.s \leftarrow A$
$K.s \leftarrow C$

$K.t \leftarrow F$
$K.t \leftarrow G$
$K.t \leftarrow H$

$K.v \leftarrow L$
$K.v \leftarrow M$
$K.v \leftarrow N$

$J.s \leftarrow J$

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 **2b** One of the underlying assumptions of Trust Management we have broadly discussed during the class is that "peers may not be continuously available".

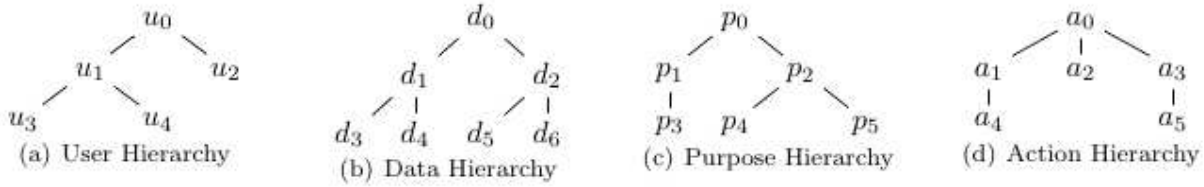
1. Explain what this means and what are the implications on the credential chain discovery system (max 7 lines)
2. Explain why is it important in a Trust Management system that "peers may not be continuously available" (max 7 lines)

Usage Control

1.5p **3** Represent the Biba model with low-watermark for objects in $UCON_{ABC}$ where integrity classes consist of an integrity level (e.g., Low, High) and a set of compartments (e.g., Financial, Administration, Research).

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 below, and $OM = (O, \rightarrow)$ is the obligation model with $O = \{o1, o2, o3, o4, o5, o6\}$ and $\rightarrow = \{o1 \rightarrow o4, o2 \rightarrow o5, q4 \rightarrow o3, o6 \rightarrow o2\}$.



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

Consider the following EPAL policies defined over Voc:

$pol_1 =$
$\langle (u_1, d_2, p_1, a_1)(+, true, \{o_1\}) \rangle$
$\langle (u_1, d_3, p_2, a_0)(\circ, true, \{o_2\}) \rangle$
$\langle (u_4, d_6, p_3, a_4)(+, true, \{o_3\}) \rangle$
$\langle (u_2, d_4, p_0, a_3)(-, true, \{o_4\}) \rangle$
$\langle (u_1, d_0, p_1, a_0)(\circ, true, \{o_5\}) \rangle$
Default ruling: $+$
Default obligations: $\{o_6\}$

$pol_2 =$
$\langle (u_1, d_2, p_1, a_1)(+, true, \{o_1\}) \rangle$
$\langle (u_1, d_3, p_2, a_0)(\circ, true, \{o_2\}) \rangle$
$\langle (u_4, d_6, p_3, a_4)(+, true, \{o_5\}) \rangle$
$\langle (u_2, d_4, p_0, a_3)(-, true, \{o_4\}) \rangle$
$\langle (u_1, d_0, p_1, a_0)(\circ, true, \{o_5\}) \rangle$
$\langle (u_0, d_0, p_0, a_0)(+, true, \{o_6\}) \rangle$
Default ruling: $-$
Default obligations: $\{o_5\}$

$pol_3 =$
$\langle (u_1, d_2, p_1, a_1)(+, true, \{o_1\}) \rangle$
$\langle (u_1, d_3, p_2, a_0)(\circ, true, \{o_5\}) \rangle$
$\langle (u_4, d_6, p_3, a_4)(+, true, \{o_3\}) \rangle$
$\langle (u_2, d_4, p_0, a_3)(-, true, \{o_4\}) \rangle$
Default ruling: $+$
Default obligations: $\{o_6\}$

1.5p **4** Determine whether:

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

Justify the answer.

Decision reduction

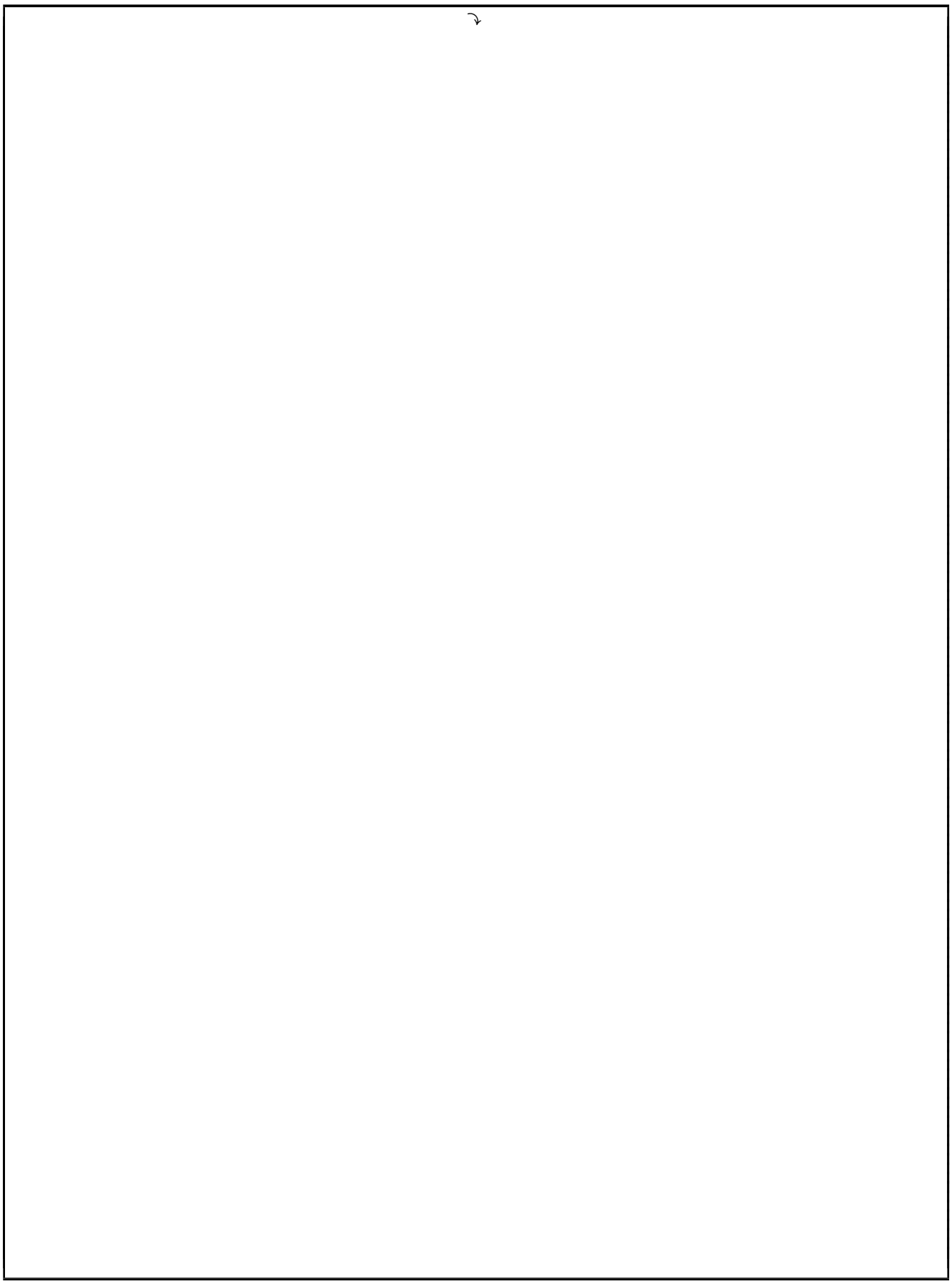
1.5p **5** Consider an access control system comprising two combining operators, α and β, defined over a four-valued decision set $D_4 = \{P, D, I, NA\}$ defined as follows:

α	P	D	I	NA
P	P	p	p	p
D	P	D	I	D
I	P	I	I	I
NA	P	D	I	NA

β	P	D	I	NA
P	P	P	P	P
D	D	D	D	D
I	I	I	I	I
NA	P	D	I	NA

1. Explain when a decision reduction is safe with respect to an operator.
2. Determine if the decision reduction ρ_{43} that maps a decision in D_4 to a decision in $D_3 = \{1, 0, \perp\}$ is safe with respect to the access control system comprising both combining operators α and β where ρ_{43} is defined as follows:

$\rho_{43}(P) = 1$
$\rho_{43}(D) = 0$
$\rho_{43}(I) = 0$
$\rho_{43}(NA) = \perp$



XACML

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

1. If MustBePresent is "False" (default value), then a missing attribute results in an empty bag (i.e., the Rule/Policy/PolicysSet is "Not Applicable").
2. 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">
                radiologist
            </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">
                PatientRecord
            </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">
                write
            </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">
               PatientRecord
           </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>
      <AnyOf>
        <AllOf>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                radiologist
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:department"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </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">
                   cardiologist
               </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="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">
                radiologist
            </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">
                14:00
            </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="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:first-applicable">
  <Target />
  <Rule Effect="Deny" RuleId="R3">
    <Target>
      <AnyOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                radiologist
            </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="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">
               radiologist
           </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">
               14:00
           </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="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">
              radiologist
           </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>
    <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>
```