

**Exercises**

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Surname, First name

---

**2IMS25 Principles of data protection**  
 Resit exam

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

a	<input checked="" type="checkbox"/>	c	d	e	f	→ b
a	b	<input checked="" type="checkbox"/>	d	e	f	→ c
<input checked="" type="checkbox"/>	b	c	<input checked="" type="checkbox"/>	e	f	→ a

Answer multiple-choice questions as shown in the example.

**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: 31/1/2024

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

**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!**

## Mandatory Access Control

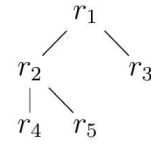
- 2p 1 Represent the Chinese Wall model in the BLP model. Specifically:
- Define a security lattice in which the Chinese Wall policy can be enforced.
  - Show how the simple-property and star-property defined by Chinese Wall model can be modeled over such a lattice structure.



**RBAC**

The following access matrix has been generate from an  $RBAC_1$  policy with the given role hierarchy and where David has role  $r_5$ .

	Client Report	Loan Offer	Financial Report
Alice	read	make	read
Bob	read		read
Charlie	read	make	
David	read write		
Eve		make	



- 1p **2** Give the minimal User-Assignment and Permission-Assignment corresponding to the given Access Matrix such that you do not assign anything that can be already derived otherwise.

**Hint:** Users might have more than one role.



**RT**

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

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

$$A.t \leftarrow K.t$$

$$K.t \leftarrow L.t \cap M.t$$

$$L.t \leftarrow Y$$

$$L.t \leftarrow Z$$

$$L.t \leftarrow W$$

$$M.t \leftarrow W$$

$$M.t \leftarrow A.t$$

$$W.t \leftarrow E$$

$$W.t \leftarrow D$$

$$W.s \leftarrow E$$

$$W.s \leftarrow L$$

$$E.s \leftarrow M$$

$$E.s \leftarrow H$$

$$E.t \leftarrow W$$

$$Z.s \leftarrow Z$$

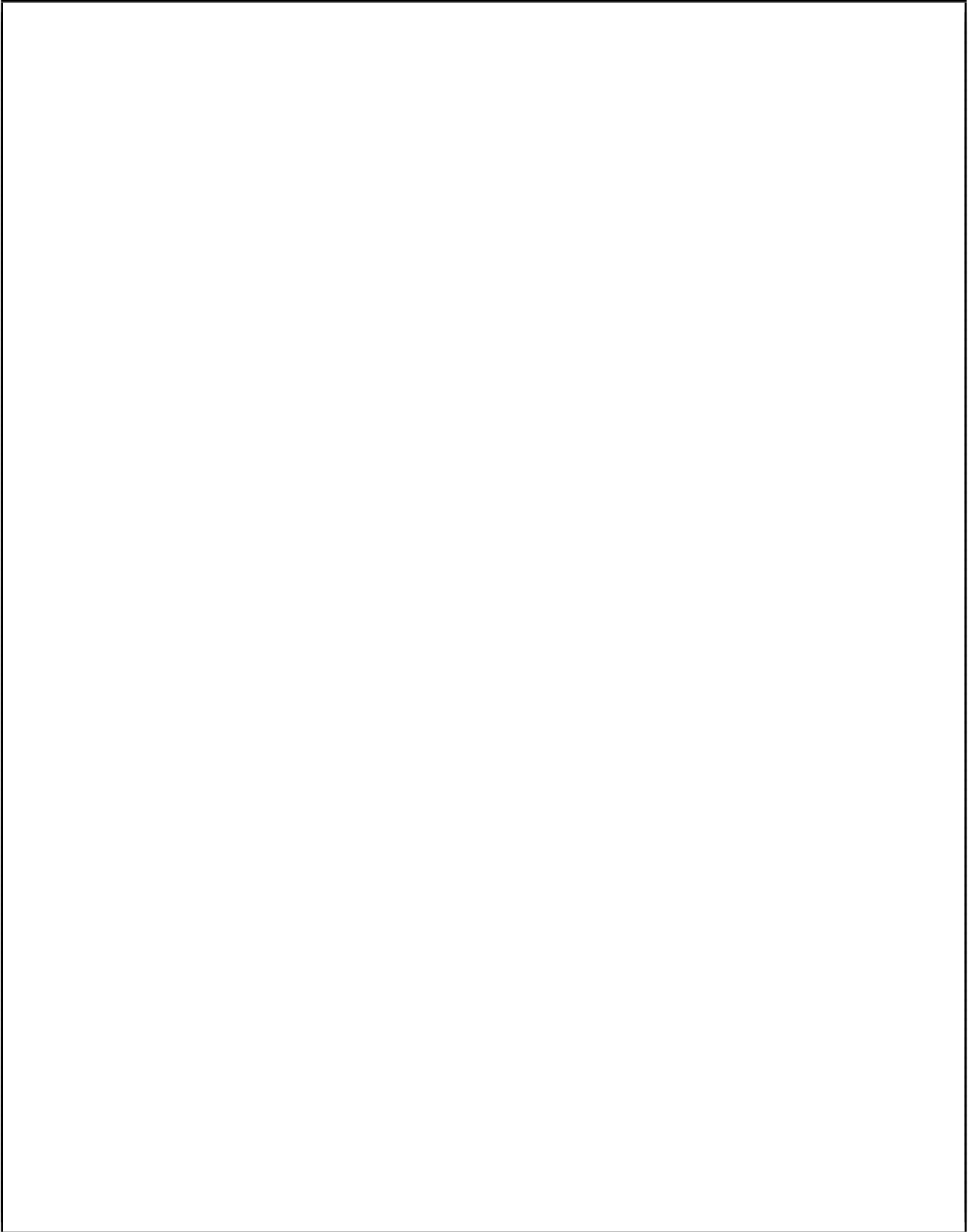
$$Z.s \leftarrow W$$

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** Explain the need to have "Trust Negotiation". Give an example in which trust negotiation is needed.



## 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.



### Decision reduction

Consider an operator defined over the three-valued decision set  $D_3 = \{1, 0, \perp\}$  defined as follows:

$\alpha$	1	0	$\perp$
1	1	$\perp$	1
0	$\perp$	0	0
$\perp$	1	0	$\perp$

- 1.5p **5**
1. Define  $\alpha$  over a seven-valued decision set  $D_7$  point-wise (Recall  $D_7 = \mathcal{P}(D_3)$ ).
  2. Explain when a decision reduction is safe with respect to an operator.
  3. Let  $D_6 = \{P, D, NA, I(P), I(D), I(PD)\}$  be a six-valued decision set and  $\rho_{76} : D_7 \rightarrow D_6$  be a decision reduction that maps a decision in  $D_7$  to a decision in  $D_6$  such that

$\rho_{76}(d) =$	$P$ if $d = \{1\}$
	$D$ if $d = \{0\}$
	$NA$ if $d = \{\perp\}$
	$I(P)$ if $d = \{1, \perp\}$
	$I(D)$ if $d = \{0, \perp\}$
	$I(PD)$ if $d = \{1, 0\}$ or $d = \{1, 0, \perp\}$

Determine whether  $\rho_{76}$  is safe with respect to  $\alpha$ .

↪



**XACML**

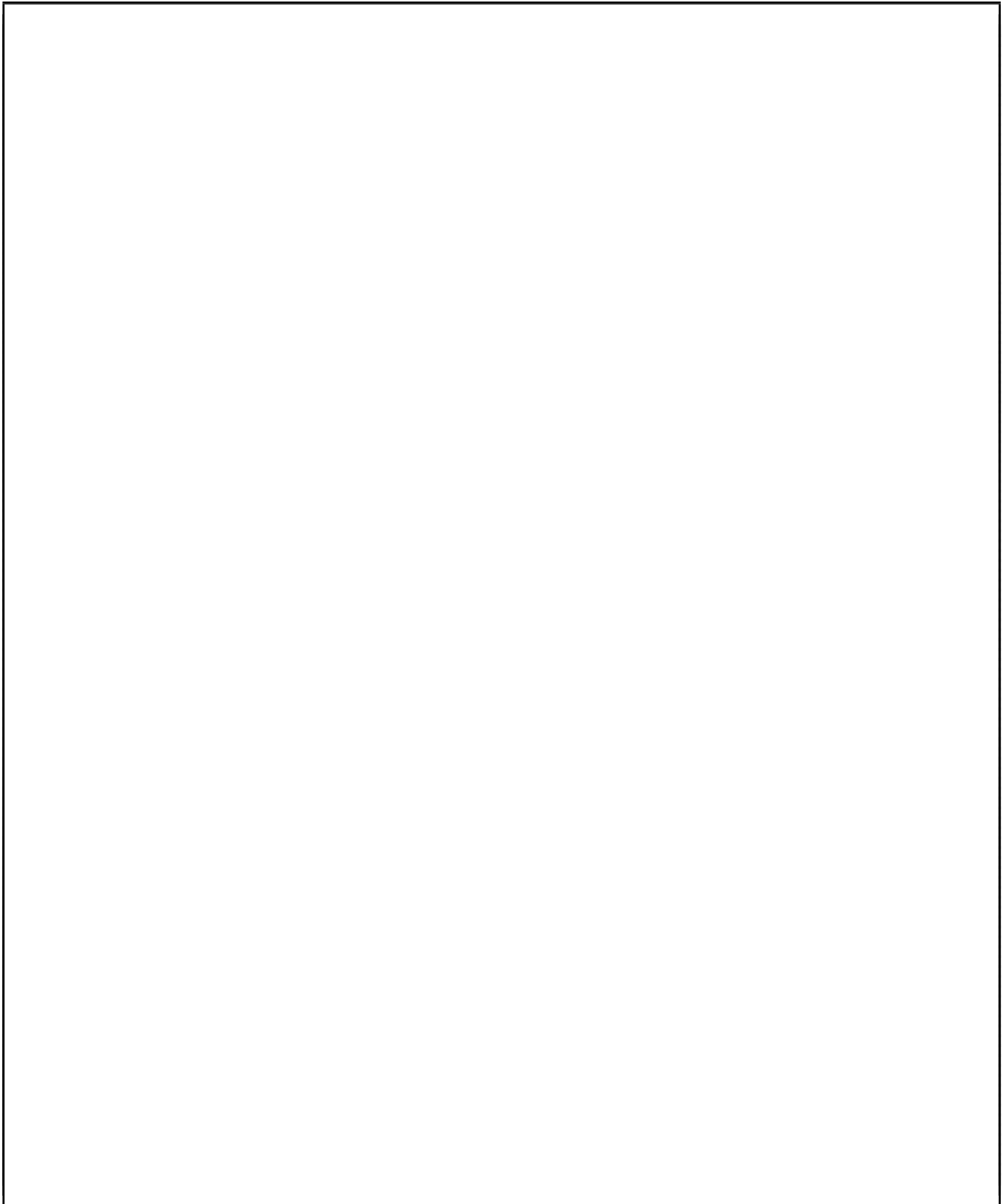
- 2p **6** Given the XACML policy and access request in attachment, determine the access response. Provide the policy graph illustrating the evaluation.

**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/PolicySet 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 had not occurred in the evaluation.

**Extra space**

7



```

<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 />
  <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">
                FinancialRecord
              </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>
      <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">
                    manager
                  </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: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">
                    read
                  </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>
            <AllOf>
              <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>
  <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="false"
      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: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>
      <AllOf>
        <Match>
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              customer service
            </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:department"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
<Rule Effect="Deny" 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">
              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>
        <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="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">
      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">
      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>
<AllOf>
  <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>
<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>

```



## 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>
  </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">
        FinancialRecord
      </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>
```