Exercises

1	2	3	4	5	6	7

Surname, First name

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

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 a document number. You can find the correct number on the top of the first page of your exam (10 numbers).

Please read the following information carefully:
Date exam: 01/02/2023
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:
No aids are allowed.

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

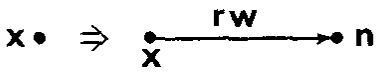
First-year bachelor students: The final grade for this exam will be announced no later than fifteen working days after the date of this exam, unless this exam takes place in Q4 or the interim period. For Q4 final exams, grades will be announced within five working days after the end of the Q4 final test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

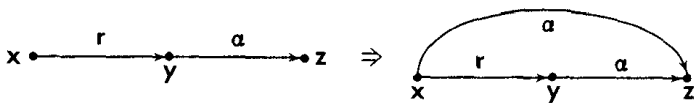
Discretionary Access Control

The Take-Grant system is an access control model that helps determining the rights (e.g., read (r) and write (w)) in a computer system. The Take-Grant system models a protection system which consists of a set of states and state transitions. The states of the protection system are modeled as directed labeled graphs, where vertices are users and the label indicates the rights that the source of the edge has over the destination. State transitions are modeled as graph rewriting rules describing admissible changes of the graph. These rules are:

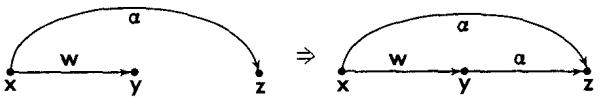
- ***Create***: Let x be a node in the graph G. The *create* rule allows one to add a new node n and an edge from x to n with label $\{r, w\}$, yielding a new graph G'. Intuitively, x creates a new user that it can *read* and *write*. This rule can be graphically represented as:



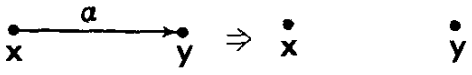
- ***Take:*** Let x, y and z be three distinct nodes in the graph G, and let there be an edge from x to y with label γ such that $r \in \gamma$ and an edge from y to z with some label $\alpha \subseteq \{r, w\}$. The *take* rule allows one to add an edge from x to z with label α, yielding a new graph G'. Intuitively, x *takes* the ability to do α to z from y. This rule can be graphically represented as:



- ***Grant***: Let x, y and z be three distinct nodes in the graph G, and let there be an edge from x to y with label γ such that $w \in \gamma$ and an edge from x to z with some label $\alpha \subseteq \{r, w\}$. The *grant* rule allows one to add an edge from y to z with label α, yielding a new graph G'. Intuitively, x *grants* y the ability to do α to z. This rule can be graphically represented as:



- ***Remove***: Let x and y be two distinct nodes in the graph G, with an edge from x to y with label γ. The *remove* rule allows one to remove the edge from x to y, yielding a new graph G'. Intuitively, x *removes* its rights to y. This rule can be graphically represented as:



1.5p **1** Construct an authorization system in Harrison-Ruzzo-Ullman model which simulates the Take-grant model. In particular, use the primitive operations provided by the Harrison-Ruzzo-Ullman model to specify commands corresponding to the rewriting rules in the Take-Grant system.

Chinese Wall

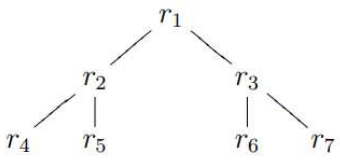
1.5p **2**

1. Explain the goal of the Chinese Wall model and describe the main concepts and properties of the model.
2. Explain the main differences between the Chinese Wall model and the Bell-LaPadula model.

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 Record	Financial Report	Loan Offer
Alice		read	read, write
Bob	read, write	read	
Charlie		read	read, review
David	read	read, write	
Eve	read	read	read, write
Frank	read, write	read	read



1.5p **3** 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 **4a** Think of a situation (i.e., a policy) in which you need to use "attribute based delegation", explain the situation in plain English, and then write a set of clauses in RT_0 modeling that situation.

1p **4b** Consider the following RT_0 policy.

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

$C.t \leftarrow J$
$C.t \leftarrow K$

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

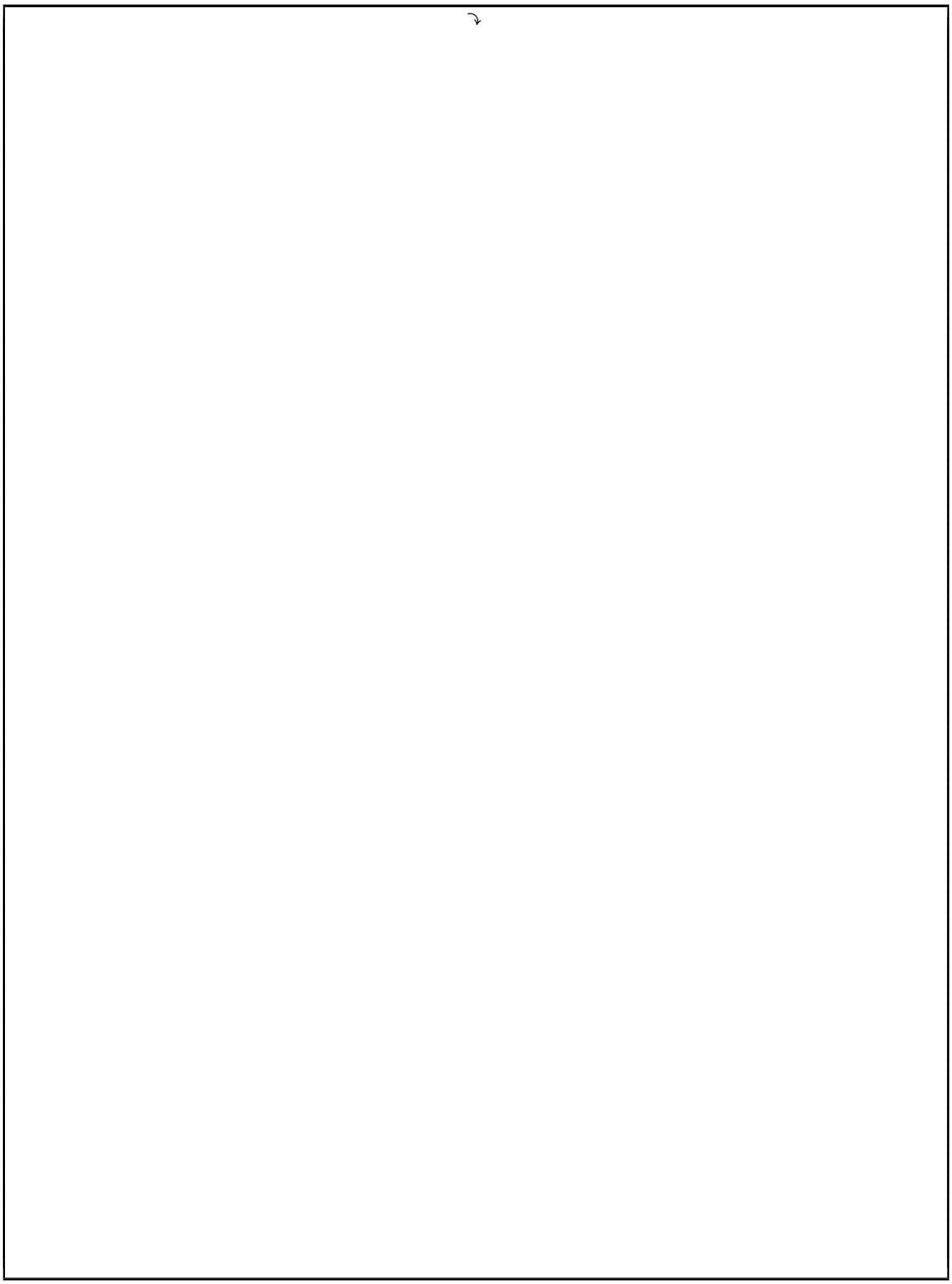
$K.s \leftarrow A$
$K.s \leftarrow B$
$K.s \leftarrow C$

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

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

$J.s \leftarrow J$

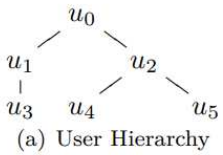
- Find all principals populating $A.t$ (which means, compute $[[A.t]]$).
- Write down the graph generated by the top-down algorithm when computing the semantics of $A.t$. (the top-down algorithm is also known as the "backward algorithm").



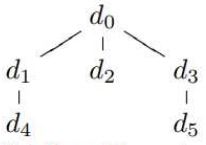
EPAL

Let pol be an EPAL policy defined over the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy reported below.

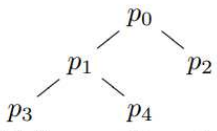
$$pol = \begin{cases} \langle (u_0, d_2, p_2, a_6)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_0)(\circ, true, \{o_2\}) \rangle \\ \langle (u_4, d_1, p_3, a_1)(+, true, \{o_3\}) \rangle \\ \langle (u_3, d_4, p_0, a_3)(-, true, \{o_4\}) \rangle \\ \langle (u_2, d_4, p_1, a_0)(\circ, true, \{o_5\}) \rangle \\ \text{Default ruling: } - \\ \text{Default obligations: } \{o_6\} \end{cases}$$



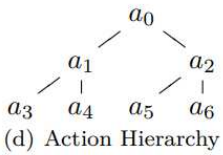
(a) User Hierarchy



(b) Data Hierarchy



(c) Purpose Hierarchy



(d) Action Hierarchy

1.5p **5** Evaluate the following access requests against pol:

$req1 = (u_3, d_5, p_4, a_6)$
$req2 = (u_1, d_0, p_3, a_1)$
$req3 = (u_4, d_4, p_5, a_3)$
$req4 = (u_2, d_4, p_3, a_4)$

XACML

2p **6** Given the XACML policy and access request below, 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.

- 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

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">
                Eve
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                clerk
            </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">
                FinancialtRecord
            </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:deny-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">
               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>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny">
    <Target>
      <AnyOf>
        <AllOf>
            <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>
    </Target>
    <Rule Effect="Deny" 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="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="Deny" 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">
                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="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>
  <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>
    <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>
    </AllOf>
  </AnyOf>
</Target>
<Rule Effect="Permit" 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">
                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>
      </AllOf>
    </AnyOf>
    <AnyOf>
      <AllOf>
        <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="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">
                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:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 financial
             </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>
  <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">
                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>
    </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>
```