Policy 1a(GPMS - no users):

Prompt:

On college campuses, several only particular faculty members are eligible to create a proposal, called PDSWhole. Only Research Faculty, Tenured Track Faculty, and Tenured Faculty can create proposals and are eligible to be PI, CoPI, and SP of the proposal. Adjunct Faculties can only be SP, Clinical and Teaching faculty can be CoPI.

Policy:

create policy class "EligibilityPolicyClass”;create user attribute "ResearchFaculty" in ["EligibilityPolicyClass "];create user attribute " TenuredTrackFaculty " in ["EligibilityPolicyClass "];create user attribute " TenuredFaculty " in ["EligibilityPolicyClass "];create user attribute " AdjunctFaculty " in ["EligibilityPolicyClass "];create user attribute " ClinicalFaculty " in ["EligibilityPolicyClass "];create user attribute " TeachingFaculty " in ["EligibilityPolicyClass "]; create object attribute "PDSWhole" in ["UniversityPolicy"]; associate "ResearchFaculty" and "PDSWhole" with ["submit"];associate "TenuredTrackFaculty" and "PDSWhole" with ["submit"]; associate "TenuredFaculty" and "PDSWhole" with ["submit"];

Policy 1b(GPMS - Users):

Prompt:

On college campuses, several only particular faculty members are eligible to create a proposal, called PDSWhole. Only Research Faculty, Tenured Track Faculty, and Tenured Faculty can create proposals and are eligible to be PI, CoPI, and SP of the proposal. Adjunct Faculties can only be SP, Clinical and Teaching faculty can be CoPI. Bob and Michelle are Adjunct Faculties, Ashley is Research Faculty, David and Dorothy are Tenured Track Faculty, Jessica is Tenured faculty

Policy:

create policy class "EligibilityPolicyClass”;create user attribute "ResearchFaculty" in ["EligibilityPolicyClass "];create user attribute " TenuredTrackFaculty " in ["EligibilityPolicyClass "];create user attribute " TenuredFaculty " in ["EligibilityPolicyClass "];create user attribute " AdjunctFaculty " in ["EligibilityPolicyClass "];create user attribute " ClinicalFaculty " in ["EligibilityPolicyClass "];create user attribute " TeachingFaculty " in ["EligibilityPolicyClass "]; create object attribute "PDSWhole" in ["UniversityPolicy"]; associate "ResearchFaculty" and "PDSWhole" with ["submit"];associate "TenuredTrackFaculty" and "PDSWhole" with ["submit"]; associate "TenuredFaculty" and "PDSWhole" with ["submit"];create user "Bob" in ["AdjunctFaculties"];create user "Bob" in

["AdjunctFaculties"];create user "Michelle" in ["AdjunctFaculties"]; create user "Ashley" in ["ResearchFaculty"];create user "David" in ["TenuredTrackFaculty"]; create user "Dorothy" in ["TenuredTrackFaculty"]; create user "Jessica" in ["TenuredFaculty"];

Policy 2a(IT Company – no users):

Prompt:

In an IT company, different users have different permissions on several objects. Quality Assurance workers can print objects from UserDatabase; Cloud Specialists can move objects in User Database. Cyber Security Experts can archive System Log objects.

Policy:

create policy class "ITPolicyClass";create user attribute "ITCoordinator" in ["ITPolicyClass"];create user attribute "CyberSecurityExpert" in ["ITPolicyClass"];create user attribute "QualityAssurance" in ["ITPolicyClass"];create user attribute "CloudSpecialist" in ["ITPolicyClass"]; create object attribute "UserDatabase" in ["ITPolicyClass"];create object attribute "SystemLog" in ["ITPolicyClass"]; associate "QualityAssurance" and "UserDatabase" with ["print"];associate "CloudSpecialist" and "UserDatabase" with ["move"];associate "CyberSecurityExpert" and "SystemLog" with ["archive"];

Policy 2b(IT Company - users):

Prompt:

In an IT company, different users have different permissions on several objects. Quality Assurance workers can print objects from UserDatabase; Cloud Specialists can move objects in User Database. Cyber Security Experts can archive System Log objects. Jessica occupies ITCoordinator; Ashley is a member of CyberSecurityExpert; David is in QualityAssurance

Policy:

create policy class "ITPolicyClass";create user attribute "ITCoordinator" in ["ITPolicyClass"];create user attribute "CyberSecurityExpert" in ["ITPolicyClass"];create user attribute "QualityAssurance" in ["ITPolicyClass"];create user attribute "CloudSpecialist" in ["ITPolicyClass"]; create object attribute "UserDatabase" in ["ITPolicyClass"];create object attribute "SystemLog" in ["ITPolicyClass"]; create user "Jessica" in ["ITCoordinator"];create user "Ashley" in ["CyberSecurityExpert"];create user "David" in ["QualityAssurance"]; associate "QualityAssurance" and "UserDatabase" with

["print"];associate "CloudSpecialist" and "UserDatabase" with ["move"];associate "CyberSecurityExpert" and "SystemLog" with ["archive"];

Policy 3a(LawFirm – no users):

Prompt:

In a lawfirm, several members can do different actions on legal objects. Attorneys can read/write legal cases. Lead Attorneys can create and delete cases. Interns can read cases. The firm has 3 offices

Policy:

create policy class "LawFirmPolicyClass"; create user attribute "Attorneys" in ["LawFirmPolicyClass"]; create user attribute "LeadAttorneys" in ["LawFirmPolicyClass"]; create user attribute "Interns" in ["LawFirmPolicyClass"]; create object attribute "LegalCases" in ["LawFirmPolicyClass"]; create object attribute "Office1" in ["LawFirmPolicyClass"];create object attribute "Office2" in ["LawFirmPolicyClass"];create object attribute "Office3" in ["LawFirmPolicyClass"];assign "LegalCases" to ["Office1"];assign "LegalCases" to ["Office2"];assign "LegalCases" to ["Office3"]; associate "Attorneys" and "LegalCases" with ["read", "write"];associate "LeadAttorneys" and "LegalCases" with ["create", "delete"];associate "Interns" and "LegalCases" with ["read"];

Policy 3b(LawFirm – users):

Prompt:

In a lawfirm, several members can do different actions on legal objects. Attorneys can read/write legal cases. Lead Attorneys can create and delete cases. Interns can read cases. The firm has 3 offices. Bob is a lead attorney, Sheryl is an attorney, and Christine is an intern.

Policy:

create policy class "LawFirmPolicyClass"; create user attribute "Attorneys" in ["LawFirmPolicyClass"]; create user attribute "LeadAttorneys" in ["LawFirmPolicyClass"]; create user attribute "Interns" in ["LawFirmPolicyClass"]; create object attribute "LegalCases" in ["LawFirmPolicyClass"]; create object attribute "Office1" in ["LawFirmPolicyClass"];create object attribute "Office2" in ["LawFirmPolicyClass"];create object attribute "Office3" in ["LawFirmPolicyClass"];assign "LegalCases" to ["Office1"];assign "LegalCases" to ["Office2"];assign "LegalCases" to ["Office3"]; associate "Attorneys" and "LegalCases" with ["read", "write"];associate "LeadAttorneys" and "LegalCases" with ["create", "delete"];associate "Interns" and "LegalCases" with ["read"];

create user " Sheryl" in ["Attorneys"];create user "Bob" in ["LeadAttorneys"];create user "Christine" in ["Interns"]; assign "Sheryl" to ["Office1"];assign "Bob" to ["Office2"]; assign "Christine" to ["Office3"];

Policy 4a(Sales – no users)

Prompt:

Access control for protecting sales data, inventory, and customer information. Sales Managers have full control over sales data, allowing them to read, write, create, and delete. Inventory Managers have full control over inventory data, allowing them to read, write, create, and delete. Customer Service can read and write customer information but are restricted from creating or deleting to prevent accidental data loss or breaches. Auditors have read-only access to all types of data, ensuring they can perform audits without modifying any data.

Policy:

create policy class "SalesManagementPolicy"; create user attribute "SalesManagers" in ["SalesManagementPolicy"]; create user attribute "InventoryManagers" in ["SalesManagementPolicy"]; create user attribute "CustomerService" in ["SalesManagementPolicy"]; create user attribute "Auditors" in ["SalesManagementPolicy"]; create object attribute "SalesData" in ["SalesManagementPolicy"]; create object attribute "InventoryData" in ["SalesManagementPolicy"]; create object attribute "CustomerInformation" in ["SalesManagementPolicy"]; associate "SalesManagers" and "SalesData" with ["Read", "Write", "Create", "Delete"]; associate "InventoryManagers" and "InventoryData" with ["Read", "Write", "Create", "Delete"]; associate "CustomerService" and "CustomerInformation" with ["Read", "Write"]; associate "Auditors" and "SalesData" with ["Read"]; associate "Auditors" and "InventoryData" with ["Read"]; associate "Auditors" and "CustomerInformation" with ["Read"];

Policy 4b(Sales – users)

Prompt:

Access control for protecting sales data, inventory, and customer information. Sales Managers have full control over sales data, allowing them to read, write, create, and delete. Bob is a sales manager. Inventory Managers have full control over inventory data, allowing

them to read, write, create, and delete. Alice is an inventory manager. Customer Service can read and write customer information but are restricted from creating or deleting to prevent accidental data loss or breaches. Auditors have read-only access to all types of data, ensuring they can perform audits without modifying any data. Christine is an auditor.

Policy:

create policy class "SalesManagementPolicy"; create user attribute "SalesManagers" in ["SalesManagementPolicy"]; create user attribute "InventoryManagers" in ["SalesManagementPolicy"]; create user attribute "CustomerService" in ["SalesManagementPolicy"]; create user attribute "Auditors" in ["SalesManagementPolicy"]; create object attribute "SalesData" in ["SalesManagementPolicy"]; create object attribute "InventoryData" in ["SalesManagementPolicy"]; create object attribute "CustomerInformation" in ["SalesManagementPolicy"]; associate "SalesManagers" and "SalesData" with ["Read", "Write", "Create", "Delete"]; associate "InventoryManagers" and "InventoryData" with ["Read", "Write", "Create", "Delete"]; associate "CustomerService" and "CustomerInformation" with ["Read", "Write"]; associate "Auditors" and "SalesData" with ["Read"]; associate "Auditors" and "InventoryData" with ["Read"]; associate "Auditors" and "CustomerInformation" with ["Read"]; create user "Bob" in ["SalesManagers"]; create user "UserInventoryManager1" in ["InventoryManagers"]; create user "Alice" in ["CustomerService"]; create user "Christine" in ["Auditors"];

Policy 5a(Health Data – no users)

Prompt:

This policy is designed to manage patient records, medical histories, and prescription details with strict access controls to ensure patient confidentiality and compliance with health data regulations such as HIPAA. The roles are divided into Doctors, Nurses, Pharmacists, and Administrators, with specific access rights assigned to each role to ensure proper handling of sensitive health data.

Policy:

create policy class "HealthDataManagementPolicy"; create user attribute "Doctors" in ["HealthDataManagementPolicy"]; create user attribute "Nurses" in ["HealthDataManagementPolicy"]; create user attribute "Pharmacists" in ["HealthDataManagementPolicy"]; create user attribute "Administrators" in ["HealthDataManagementPolicy"]; create object attribute "PatientRecords" in ["HealthDataManagementPolicy"]; create object attribute "MedicalHistories" in ["HealthDataManagementPolicy"]; create object attribute "PrescriptionDetails" in

["HealthDataManagementPolicy"]; associate "Doctors" and "PatientRecords" with ["Read", "Write", "Create", "Delete"]; associate "Doctors" and "MedicalHistories" with ["Read", "Write", "Create", "Delete"]; associate "Doctors" and "PrescriptionDetails" with ["Read", "Write", "Create", "Delete"]; associate "Nurses" and "PatientRecords" with ["Read", "Write"]; associate "Nurses" and "MedicalHistories" with ["Read", "Write"]; associate "Nurses" and "PrescriptionDetails" with ["Read"]; associate "Pharmacists" and "PrescriptionDetails" with ["Read", "Write"]; associate "Administrators" and "PatientRecords" with ["Read"]; associate "Administrators" and "MedicalHistories" with ["Read"]; associate "Administrators" and "PrescriptionDetails" with ["Read"];

Policy 5b(Health Data – users)

Prompt:

This policy is designed to manage patient records, medical histories, and prescription details with strict access controls to ensure patient confidentiality and compliance with health data regulations such as HIPAA. The roles are divided into Doctors, Nurses, Pharmacists, and Administrators, with specific access rights assigned to each role to ensure proper handling of sensitive health data. Each user attributes should have a default user.

Policy:

create policy class "HealthDataManagementPolicy"; create user attribute "Doctors" in ["HealthDataManagementPolicy"]; create user attribute "Nurses" in ["HealthDataManagementPolicy"]; create user attribute "Pharmacists" in ["HealthDataManagementPolicy"]; create user attribute "Administrators" in ["HealthDataManagementPolicy"]; create object attribute "PatientRecords" in ["HealthDataManagementPolicy"]; create object attribute "MedicalHistories" in ["HealthDataManagementPolicy"]; create object attribute "PrescriptionDetails" in ["HealthDataManagementPolicy"]; associate "Doctors" and "PatientRecords" with ["Read", "Write", "Create", "Delete"]; associate "Doctors" and "MedicalHistories" with ["Read", "Write", "Create", "Delete"]; associate "Doctors" and "PrescriptionDetails" with ["Read", "Write", "Create", "Delete"]; associate "Nurses" and "PatientRecords" with ["Read", "Write"]; associate "Nurses" and "MedicalHistories" with ["Read", "Write"]; associate "Nurses" and "PrescriptionDetails" with ["Read"]; associate "Pharmacists" and "PrescriptionDetails" with ["Read", "Write"]; associate "Administrators" and "PatientRecords" with ["Read"]; associate "Administrators" and "MedicalHistories" with ["Read"]; associate "Administrators" and "PrescriptionDetails" with ["Read"]; create user "UserDoctor" in ["Doctors"]; create user

"UserNurse" in ["Nurses"]; create user "UserPharmacist" in ["Pharmacists"]; create user "UserAdministrator" in ["Administrators"];