Политики безопасности

Раздел **Policies** (`/policies`) управляет правилами доступа агентов (OPA/Rego + шаблоны соответствия).

> **Минимальные роли**
>
> `Чтение — Developer / Security Analyst+. Создание и изменение — **Admin+**.`

Список политик

Колонки: Name, Severity (`low` … `critical`), Status (Active), Default, Actions (Edit / Delete).

Создание политики

1. Нажмите **Create Policy**.
2. Выберите шаблон из каталога (`GET /api/v1/policies/templates`):

Шаблон	Типичная severity	Назначение
`gdpr`	Critical	Персональные данные (EU)
`hipaa`	Critical	Медицинские данные (US)
`fz152`	Critical	Персональные данные (РФ, ФЗ-152)
`hitl`	High	Требование ручного согласования
`custom`	Medium	Свои правила

1. Заполните Name, Description, Severity, Rules (JSON/Rego в редакторе).
2. Включите **Active** (и при необходимости **Default**).
3. **Save**. Редактирование: `/policies/:id` .

> **Юридическая оговорка**
>
> `Шаблоны GDPR / HIPAA / ФЗ-152 — стартовая база для инженерии контроля, а не юридическая сертификация. Финальную валидацию делает комплаенс вашей организации.`

Проверка действия (Policy Check)

Перед опасной операцией агент/интеграция вызывает:

```
curl -X POST http://localhost:8001/api/v1/policies/check \
  -H "X-API-Key: $TENANT_API_KEY" \
  -H "Content-Type: application/json" \
  -d '{
    "agent_id": "'"$AGENT_ID"'",
    "action": "export_data",
    "resource": "customers",
    "context": {}
  }'
```

В ответе смотрите: `allowed`, `reason`, `severity`, `required_approval`, `risk_score`, признаки anomaly.

- `allowed=false` → событие `policy.violated`, запись в Audit.
- `required_approval=true` → путь через **HITL**.

Операторский цикл

1. Получили toast / запись о нарушении.
2. Найдите событие в **Audit**.
3. Откройте соответствующую политику в **Policies**.
4. Решите: ошибка контекста агента, нужна HITL, или политика слишком жёсткая/мягкая (меняет Admin).
5. Зафиксируйте вывод для команды.

Подробнее (EN): Policies.