

Innofactor Incident Response Matrix

Customer: Verdis
Last update: {{TODAY}}

Response

| Category | Action | Permissions needed | Playbook | Verdis | Innofactor |
|-----------|---------------------------------|---|---|-------------------|------------|
| Entra ID | Revoke user sessions | Helpdesk Administrator | <input checked="" type="checkbox"/> Deployed | Informed in teams | Allowed |
| | Reset user password | Helpdesk Administrator | <input checked="" type="checkbox"/> Deployed | Informed in teams | Allowed |
| | Block EntraID user | | ✗ | - | - |
| Email | Soft delete emails | Unified RBAC Email & collaboration advanced actions (manage) | | | Allowed |
| | Hard delete emails | Unified RBAC Email & collaboration advanced actions (manage) | | | Allowed |
| | Read email content | Unified RBAC Email & collaboration content (read) | | Informed in teams | Allowed |
| Endpoints | Run quick Antivirus scan | Security Administrator | <input checked="" type="checkbox"/> Deployed | Informed in teams | Allowed |
| | Isolate/release infected device | Security Operator | <input checked="" type="checkbox"/> Deployed | Informed in teams | Allowed |
| | Live response | Unified RBAC Basic / Advanced live response (manage) | | Informed in teams | Allowed |

Additional Actions

| Action | Permissions needed | Verdis | Innofactor |
|-----------------------------------|------------------------|-------------|-------------|
| Contact with end users | | Responsible | |
| Updating tenant allow / blocklist | Security Administrator | Responsible | Responsible |
| Restore isolated users / devices | | Responsible | |