CYBERSECURITY

# Safeguarding OCWA-managed Systems

## As a water and wastewater services provider, ensuring the security of OCWA's technology infrastructure and data is a key priority.

OCWA is guided by the leading security frameworks and also receives regular notifications from many expert sources.

Our cybersecurity experts safeguard OCWA's IT, Supervisory Control and Data Acquisition (SCADA) systems, technology infrastructure, and the data that we manage from cyber threats.

OCWA's cybersecurity system safeguards include advanced technology to detect and protect against threats to OCWA's network infrastructure and assets. This is to protect OCWA-owned computers, networks and other assets at client facilities before, during and after cybersecurity events. We also encourage clients to take their own appropriate security measures regarding their facilities and assets.


### We follow industry best practices and additional procedures as required of a Crown Agency, including:

- Hiring expert IT personnel dedicated to strengthening the security and resilience of our network infrastructure and protecting client data that we manage
- Implementing multiple layers of defense and proactive security controls to thwart, mitigate, and effectively respond to evolving cyber threats
- Undertaking regular risk management reviews
- Maintaining a cycle of continuous improvement, regular security upgrades, and security awareness education and training for our staff


**For more information, contact:**
**Eric Dorman** | Vice-President, Information & Information Technology, OCWA
edorman@ocwa.com www.ocwa.com

ONTARIO CLEAN WATER AGENCY
AGENCE ONTARIENNE DES EAUX

## Security in mind

**Knowing what to look for is critical in choosing IT systems and tools.**

OCWA reviews applications and updates from many angles, including logical and physical cybersecurity controls. Our enterprise systems such as Process Data Management (PDM), Work Management System (WMS) and SCADA systems were developed and customized with security features.

These include:

- Implementing Identity and Access Management throughout the account management lifecycle. Privileges are granted to users on a need-to-know basis. Users are assigned only the privileges they need to perform their job.
- Employing “default to fail secure.” An application or system failure will cause little or no harm to other systems.
- Applying multiple layers of defense including:
  - Intrusion detection systems constantly monitoring traffic flow (borders)
  - Firewalls that provide real-time filtering
  - Cryptography and layered authentication (zones)
  - Certified professionals ensuring system integrity (gatekeepers)
- Constant monitoring and tracking for quick and effective response to attacks
- Performing routine vulnerability scans and threat assessments
- Carrying out periodic cybersecurity audits and risk compliance checks
- In the event of an external breach in any of our systems, OCWA utilizes a “Vault Solution” offsite backup to ensure quick operational recovery. This remote backup site – accessible only by specific OCWA staff – ensures that secure backups are performed regularly to reduce risk.

***Get in touch to learn more.***

## Our security measures

### Perimeter Firewalls

Advanced devices that detect and prevent network intrusions through real-time traffic analysis and provide advanced protection against malware.

### Server Network Firewalls

Firewalls that recognize whether files are considered safe and sends unknown files through multiple layers of security.

### VPN and Local Firewalls

VPN and Local Operations Firewalls that allow us to restrict access at the local level.

### Access Barriers

Access checkpoints that result in highly configured rights for user accounts and follow the principle of least privilege — user access is strictly granted at a minimum level.

### Privilege

Users assigned to different privilege groups depending on their access to data.

### Design

Secure design of PDM, Maximo, SCADA.

### Disaster Recovery

Multi-layered Disaster Recovery Systems with automatic and manual failovers.

### Experts

People who control and monitor systems and lock them down in response to security threats.

### Commitment

OCWA’s commitment to security.