AU CHÂTEAU
Une résidence de choix · A residence of choice

Appendix P

CODE GREY

Policy

At Au Château, **essential services** include, but are not limited to:

- Heating, ventilation, and air conditioning system.
- Electrical power and emergency lighting
- Fire detection, alarm, and life-safety systems.
- Communication and response system.
- Elevators.
- Safety and emergency equipment.
- Water and sewage system.
- Information and cybersecurity systems

Au Château will have contingencies in place for planned or unanticipated loss of essential services ensuring the daily operation of the site with minimal disruption.

Purpose

The purpose of this policy is to ensure the continuity of essential services at Au Château and to protect the health, safety, dignity, and well-being of residents, staff, visitors, and others on site during a planned or unanticipated loss of essential services. This policy supports timely decision-making, effective communication, and coordinated response in a Long-Term Care environment.

General Information:

Loss of Power:

Fire system - loss of power may signal to the fire monitoring surveillance, system distress, or technical "trouble" signal from your annunciator panel.

- Supervisor/Designate will be required to notify the monitoring company or receive direction from the property management office, if applicable.
- In the event you do not have technical fire system support with your annunciator panel you will be required to begin a Fire Watch.

When Utilities Are Restored (If Appropriate):

- Run a building check to ensure all is safe for the return of services. Example: do an elevator run, stopping at all floors, before you have occupants use the elevator.
- Ensure the fire panel is full power and operational.

- Check with the monitoring company to be sure the system is reading correctly.
- Check to make sure all maglocks have been reset and are functioning if applicable.

Back-up mechanisms and reserves for loss of power:

- Generators on-site or rental.
- Emergency lighting.

Cybersecurity

In today's age, a cybersecurity incident is a question of "when," not "if". This policy serves as a guideline, outlining the expected conduct of individuals and delineating the appropriate and inappropriate utilization of Au Château's digital technologies and assets.

It is incumbent upon every individual to ensure that the technologies and data they use are solely for their intended purposes, and digital information stored or transferred over the network remains safeguarded against unauthorized access, use, or corruption.

This policy applies to all staff members, contractors, consultants, temporary staff members, and other workers, including all personnel affiliated with third parties. The policy encompasses a spectrum of digital assets, including but not limited to:

- **Computer Equipment**: Desktops, laptops, tablets, and servers.
- **Mobile Devices**: Smartphones and tablets.
- **Software**: Licensed and in-house developed applications.
- **Storage Media**: SSD/Hard drives, USB drives, and cloud storage.
- **Data**: Customer data, corporate data, and any other form of digital information.
- **Network Infrastructure**: Routers, switches, firewalls, and other networking hardware.
- **Network Access**: Wired and wireless connectivity to the corporate network.
- **Communication Tools**: Email and messaging platforms.
- **Internet Browsing Data**: Information collected during web browsing.
- **System Logs**: Records of system activities and transactions.
- **Credentials**: Usernames, passwords, and any other forms of authentication.

<u>Procedure</u>

1. The first person to learn of the loss of essential services will report to the Supervisor/Designate who will assume the role of Incident Commander (IC).

2. The Incident Commander Will:

- Determine if a contingency plan is required.
- Activate contingency emergency plan, if required, based on the essential service(s) lost.
- At the end of the Code Grey- complete the Code Grey-Post Incident Review and Debrief Form (see Appendix P1).

a. Power Failure:

I. The Incident Commander/Designate Will:

- Notify key personnel to 'come to work' or 'stay away from work' at the discretion of the Administrator or Designate (refer to Appendix C).
- Direct staff members to monitor all doors as security doors are now unlocked, and reset mag locks (reference Generator Policy)
- Equip staff members with flashlights, batteries, and other emergency supplies.
- Patrol the building **(Fire Watch)** and ensure there are no immediate emergencies.
- Recommend that occupants limit unnecessary activities during this time; remain in safe areas unless otherwise directed.
- Minimize the use of hot water.
- Communicate and cooperate with other community partners as may be needed to support internal or external emergency needs.

II. The Environmental Services Manager/Designate Will:

- Investigate the source of the problem and contact a certified electrical contracting service, if needed.
- Shut down all gas appliances that require a powered vent, e.g., gas ranges.
- Monitor the performance and fuel reserve for the standby generator and provide recommendations concerning potential load shedding or added fuel requirements.
- Ensure adequate temperature and water supply for occupants.
- Ensure emergency lighting supplies are operable and that a supply of backup batteries is available.
- Maintain contact with the municipality to determine the length of external power failures.

III. Food Services Will:

- Please refer to Appendix P2- Emergency Food Services Contingency Plan
- Prioritize the use of existing food supplies according to longevity
- Refrain from opening the refrigeration equipment doors as much as possible.
- Reference timing of food safety guidelines (see local Public Health website).
- Prepare to move refrigerator and freezer foods if necessary to an available source.

IV. The Director of Care will review Vaccine and Other Medication Storage and Handling:

- As soon as the power outage is noticed, the lead or the backup staff member must document the time in the logbook and record the current, minimum, and maximum temperature of vaccines and other medication in a non-functioning refrigerator.
- Inform the Supervisor/Designate immediately.

- In the case of a power outage: call the electricity service provider to gather information regarding the outage e.g.: how long the outage will be, and the specific area affected.
- Call Public Health for future instructions. Inform Public Health when the power is expected to be restored (if known). Public Health also needs to be informed if an alternate power source is used.
- If instructed to do so, by Public Health, transfer vaccines and other medication to the alternative refrigerator, another site or storage facility, or in an insulated container with appropriate packaging material and temperature monitoring devices.

V. Generator Information

All procedures related to the following are outlined in the 'Generator Testing and Maintenance Policy'. A copy of the policy, and related documentation, and the generator manual are maintained in the S:drive → Policies & Procedures →Emergency Preparedness, and in the Administrator's office.

- Generator start-up
- Operations
- Load management
- Testing
- Maintenance
- Emergency troubleshooting

VI. Failure of Emergency Generator

In the event the on-site emergency generator does not operate as expected, the Incident Commander/Designate will:

- Contact the Administrator and/or Environmental Services Manager
- Refer to Appendix D for Generator Contractor Contact Information

b. Loss of Natural Gas Supply:

I. General Information:

The site relies on its natural gas supply for some heating and hot water supply.

Areas that may be affected by a loss in the natural gas supply:

- HVAC, hot water, kitchen.
- All gas-fired kitchen equipment.
- Central heating and air system.
- Portions of the domestic hot water heating system.

All gas operated equipment, and the location of shut offs are identified in building drawings.

- The natural gas and equipment maintenance provider contact numbers are identified in the Site Profile Chart (refer to Appendix J).

II. The Incident Commander/Designate Will:

- Ensure that occupants are kept warm or cool, as required.
- Advise staff members to ensure that all exterior doors and windows are always kept closed.
- Advise staff members of alternative methods for heating water including the use of electric kettles, and microwave ovens, as required.
- Communicate the operational impact to occupants.
- Evaluate the situation if an evacuation is required.
- Contact utility company and follow the appropriate directions.

c. Loss of Air Conditioning:

I. The Incident Commander/Designate Will:

- Ensure that occupants are kept cool and comfortable.
- Advise staff members to ensure that all exterior doors and windows are kept closed.
- Advise staff members of alternative methods for cooling as required.
- Reduce interior lights to minimize heat.
- Communicate the operational impact to all occupants

II. In case of an extended absence of air conditioning in extreme heat:

- Decide to implement hot weather protocols and cancel programs, as required.
- Utilize all electrical fans (if applicable) for central corridors and open doors to initiate airflow.
- Reduce activities to avoid overheating.
- Contact family members and advise of the issue, if required.
- Determine the internal problem.
- Refer to drawings and equipment manuals for shutoffs.
- Contact service contractor to fix equipment.

d. Loss of Water Supply:

The site will maintain a supply of drinking water to be used in the case of an emergency.

I. The Incident Commander/Designate Will:

- Identify emergency water distribution priorities and contingencies for loss of water (refer to Appendix D).
- If the water supply is contaminated follow the direction of Public Health Authorities.

II. The Environmental Services Manager/Designate Will:

- Perform damage assessment

- Shut off water supply lines to all areas (excluding fire sprinkler system)
- Identify emergency water source locations.
- Verify on-hand water supplies and confirm the volume.
- Arrange for pick-up and distribution of emergency water supplies, if required.

III. Food Services Will:

Ensure Food Safety and Infection Control during emergency conditions by:

- Maintaining clean food preparation surfaces. Use disinfectant solution when required.
- Follow Hazard Analysis Critical Control Points guidelines to ensure safe food practices.
- Ensuring that prepared food does not become cross-contaminated with “non-potable” water.
- Designate staff members to assess and confine ALL food items that may have been in contact with “non-potable” water before the alert.
- Contaminated food products are to be tallied and recorded before being discarded.

IV. Designated Staff Member Will:

- Post non-drinkable water signs at all water taps within their assigned area including:
    - Common washrooms
    - Utility rooms
    - Water taps in the kitchen used for food preparation, handling, pot washing
- Follow Public Health direction in the event of a Boil Water Advisory:
    - Use water substitutes for cleansing
    - Hand sanitizers
    - Rubbing alcohol

e. Loss of Communications:

Determine whether the loss of communication services is specific to Au Château’s property or is a municipal and provincial loss of services.

- Direct staff members to use cell phones, if available.

f. Cybersecurity:

Cybersecurity procedures are crucial for protecting organizations against digital threats and ensuring the confidentiality, integrity, and availability of sensitive information and systems. Here are some key components and steps to establish effective cybersecurity procedures:

I. Staff members Responsibilities:

- Majority of cybersecurity incidents occur due to human error (phishing, weak passwords, and deceptive activities that manipulate individuals into divulging confidential or personal information, etc.)

- Ensure all technologies and data are used solely for their intended purposes.
- Safeguard digital information against unauthorized access, use, or corruption.
- Report any suspicious activity or security incidents immediately to the IT department.
- Follow all prescribed procedures for using and managing passwords and other credentials.

II. IT Department Responsibilities:

- Implement and maintain security measures to protect digital assets.
- System safeguards can offer ways of reducing the risk or impact, such as:
    - Robust and isolated backup infrastructure.
    - Full-disk encryption.
    - Strong passwords/password managers.
    - Allow and deny lists.
    - Network isolation.
    - Rule of least privilege.
- Monitor network activity and respond to security incidents.
- Patch Management: Implement procedures for timely patching and updating of software, operating systems, and applications to address known vulnerabilities and reduce the risk of exploitation by cyber attackers.
- Data Backup and Recovery: Establish backup and recovery procedures to ensure the timely and secure backup of critical data and systems, as well as the ability to recover data in the event of a cyber incident.
- Conduct regular security training and awareness programs.
- Ensure compliance with industry standards and regulations.

III. Management Responsibilities:

- Promote a culture of cybersecurity awareness training within the organization.
- Mitigation strategies should include staff member training related to technology and media literacy, phishing prevention, risk identification, and social engineering prevention.
- Provide the necessary resources and support for effective cybersecurity practices.
- Enforce compliance with this policy.
- Conduct exercises and drills for detecting, responding to, and recovering from cyber incidents such as data breaches, malware attacks, or system compromises.

.

References:

- Appendix B- Call Back Procedure & Record Sheet
- Appendix C- Staff Emergency Call List
- Appendix D- Emergency Vendor and Community Contact List

- Appendix E- Emergency Kit
- Appendix F- IMS 201 Incident Briefing
- Appendix L- Code Green
- Appendix P1- Code Grey- Post Incident Review and Debrief Form
- Appendix P2- Emergency Food Services Contingency Plan