Administration & Finance Division
Information Technology Department Report
[2020-1004]

Date: May 5th, 2020

To: Administration & Finance Executive Committee

From: Jeremy Hughes, Information Technology Manager

Subject: Coverage for Information Technology Support Services

---

Purpose

To develop coverage for Information Technology (IT) support services affecting both the *Town of Fort Frances* (*ToFF*) and the *Fort Frances Public Library Technology Centre* (*FFPLTC*) when regular staff is unavailable due to scheduled annual vacation or an extended leave of absence.

The attached document describes a mutually beneficial arrangement that will come into effect for the 2020 operating year on a trial basis. This arrangement will be subject to review before adoption in 2021, when it will be amended to the 2012 "Memorandum of Understanding" (MOU) between the *ToFF* and *FFPLTC*.

The attached document defines potentially affected systems, expected types of incidents, required levels of service, and the steps necessary to build the capacity of our available human resources to respond to each identified system and incident type.

Attachments

Attached is a document titled "Information Technology Support Services" (7 pages). It is recommended that Council approve a new trial arrangement of coverage for IT support services based on the prescriptions detailed in this document.

Approval of this report will authorize a new trial arrangement of coverage for Information Technology support services between the *Fort Frances Public Library Technology Centre* and the *Town of Fort Frances* for the 2020 operating year, subject to approval by the *Fort Frances Public Library Board*.

Information Technology Support Services

1) Purpose

To develop coverage for Information Technology (IT) support services affecting both the *Town of Fort Frances* (*ToFF*) and the *Fort Frances Public Library Technology Centre* (*FFPLTC*) when regular staff is unavailable due to scheduled annual vacation or an extended leave of absence.

Achieving comprehensive coverage for IT support services requires an understanding of potentially affected systems, expected types of incidents, and expected levels of service. Steps must be taken to build the capacity of our available human resources to respond to each identified system and incident type.

2) Human Resources

There are currently three full-time employees responsible for IT support services at the *ToFF* and *FFPLTC*:

- IT Manager (*ToFF*)
- Junior IT Specialist (*ToFF*)
- IT Coordinator (*FFPLTC*)

Both the IT Manager and Junior IT Specialist are stationed at the Civic Centre, with the IT Coordinator stationed at the *FFPLTC*.

3) Systems

Systems are classified as either critical or non-critical depending on their potential impact to business processes. Some systems are common among both the *ToFF* and *FFPLTC*. Some systems are external to *ToFF* operations but fall under the responsibility scope of the IT Manager.

The effective list of systems will be developed over time, external to this document.

4) Incidents

Incidents are classified as either critical or non-critical depending on how they affect a specific system.

The effective list of incidents will be developed over time, external to this document.

5) Levels of Service

When incidents are responded to:

- Critical incidents typically require an immediate response
- Non-critical incidents typically may be deferred to the next business day

How incidents are responded to:

- Incidents occurring during regularly scheduled work hours are responded to by the IT employee responsible for any affected systems
- Incidents occurring outside of regularly scheduled work hours are responded to by an IT employee on standby

5.1) Standby Considerations

The IT Manager is effectively on standby for all *ToFF* systems when they are scheduled to work.

When the IT Manager is not scheduled to work, either the IT Coordinator or the Junior IT Specialist will be placed on standby in order to monitor any critical incidents that may develop.

An IT employee on standby will be compensated with 1 hour for each day of standby duty performed. Such compensation may be taken as time off or as payment in addition to salary.

If an IT employee on standby responds to an incident, they will be compensated at their regular rate in accordance with Management / Non-Union Benefits Policy (3.10 section 9b):

> *"Straight time for any hours worked in excess of their regular work-week (35 or 40) up to 44 hours per week. Any hours worked in excess of 44 hours per week will accumulate at the rate of 1.5 times hours worked."*

Standby compensation will be allocated as a *ToFF* expense. Time spent responding to incidents will be allocated to the department responsible for the affected service. A minimum duration of 0.5 hours of work must be performed before time spent responding to incidents may be claimed.

5.2) Competing Responsibilities

IT employees have competing responsibilities during regularly scheduled working hours that may render them incapable of responding to a critical incident in certain scenarios. In these cases, efforts will be made to secure coverage prior to responding to a critical incident. Coverage may be obtained for the *FFPLTC* from a staff call-in list, or from the Civic Centre through coordination with the *ToFF* CAO.

6) Incident Response Duties

IT employees will remain at their regularly scheduled stations unless responding to an incident.

The availability of each employee determines who responds to an incident. There are eight possible scenarios to consider:

IT Manager (*ToFF*)	IT Coordinator (*FFPLTC*)	Junior IT Specialist (*ToFF*)	Outcome
In	In	In	• Each employee oversees their regular duties.
In	In	Out	• The IT Manager assumes the support responsibilities of the Junior IT Specialist.

IT Manager (*ToFF*)	IT Coordinator (*FFPLTC*)	Junior IT Specialist (*ToFF*)	Outcome
In	Out	In	• The IT Manager assumes the support responsibilities of the IT Coordinator on a standby basis. • Critical incidents involving *FFPLTC* systems are immediately reported to the *FFPLTC* CEO by the IT Manager. • If the IT Coordinator is reachable, the *FFPLTC* CEO decides whether to engage the IT Coordinator in the resolution of any critical incident involving *FFPLTC* systems. • Non-critical incidents involving *FFPLTC* systems may be escalated to the IT Manager by the *FFPLTC* CEO or deferred at their discretion. • Incidents involving *FFPLTC* systems may be delegated to the Junior IT Specialist by the IT Manager at their discretion.
In	Out	Out	• The IT Manager assumes the support responsibilities of the IT Coordinator and Junior IT Specialist on a standby basis. • Critical incidents involving *FFPLTC* systems are immediately reported to the *FFPLTC* CEO by the IT Manager. • If the IT Coordinator is reachable, the *FFPLTC* CEO decides whether to engage the IT Coordinator in the resolution of any critical incident involving *FFPLTC* systems. • Non-critical incidents involving *FFPLTC* systems may be escalated to the IT Manager by the *FFPLTC* CEO or deferred at their discretion.
Out	In	In	• The IT Coordinator assumes the support responsibilities of the IT Manager on a standby basis. This is an interim measure until the Junior IT Specialist achieves the operational capacity to fully assume the support responsibilities of the IT Manager on a standby basis. • Critical incidents involving *ToFF* systems are immediately reported to the *ToFF* CAO by the IT Coordinator. • If the IT Manager is reachable, the *ToFF* CAO decides whether to engage the IT Manager in the resolution of any critical incident involving *ToFF* systems. • Non-critical incidents involving *ToFF* systems may be delegated to the Junior IT Specialist by the IT Coordinator at their discretion.

IT Manager (*ToFF*)	IT Coordinator (*FFPLTC*)	Junior IT Specialist (*ToFF*)	Outcome
Out	In	Out	*This is an extreme case. The IT Manager and Junior IT Specialist will proactively schedule themselves to not be off work on the same regular workday.* • The IT Coordinator assumes the support responsibilities of the IT Manager and Junior IT Specialist on a standby basis. • Critical incidents involving *ToFF* systems are immediately reported to the *ToFF* CAO by the IT Coordinator. • If the IT Manager is reachable, the *ToFF* CAO decides whether to engage the IT Manager in the resolution of any critical incident involving *ToFF* systems.
Out	Out	In	*This is an extreme case. The IT Manager and IT Coordinator will proactively schedule themselves to not be off work on the same regular workday.* • The Junior IT Specialist assumes the support responsibilities of the IT Manager and the IT Coordinator on a standby basis. • Critical incidents involving *ToFF* systems are immediately reported to the *ToFF* CAO by the Junior IT Specialist. • If the IT Manager is reachable, the *ToFF* CAO decides whether to engage the IT Manager in the resolution of any critical incident involving *ToFF* systems. • Critical incidents involving *FFPLTC* systems are immediately reported to the *FFPLTC* CEO by the Junior IT Specialist. • If the IT Coordinator is reachable, the *FFPLTC* CEO decides whether to engage the IT Coordinator in the resolution of any critical incident involving *FFPLTC* systems. • Non-critical incidents involving *FFPLTC* systems may be escalated to the Junior IT Specialist by the *FFPLTC* CEO or deferred at their discretion.
Out	Out	Out	*This is an extreme case. Scenarios where no IT employees are available may occur if a lone scheduled employee is unexpectedly unavailable to work. Possible causes may include: illness, injury, personal matters, etc.* • The *ToFF* CAO and *FFPLTC* CEO triage any incidents with their available resources.

6.1) Designates

If the *ToFF* CAO is unavailable, their designate should be reported to instead. If the *FFPLTC* CEO is unavailable, their designate should be reported to instead. Selected designates will be proactively communicated to IT employees.

6.2) Scheduling

To achieve operational resiliency and minimize the risk associated with critical incidents, scenarios where more than one IT employee is unavailable should be avoided. IT employees will proactively schedule themselves to not be off work on the same regular workday.

Competing vacation requests may be affected and will be resolved through mutual agreement by the *FFPLTC* CEO, *ToFF* CAO, and IT Manager.

6.3) Access

All IT employees will have access to Administration vehicles through coordination with the Deputy Clerk.

7) Trial Basis

When officially approved in principle by both parties, the arrangement described in this document will come into effect on a trial basis for the 2020 operating year. This trial arrangement will be reviewed by both parties for any required adjustments prior to the finalization of operating budgets for the 2021 operating year. When officially approved for the 2021 operating year, this arrangement will be amended to the 2012 “Memorandum of Understanding” (MOU) between the *ToFF* and *FFPLTC*.

Appendix A: Implementation Requirements

A1) Payroll

- Establish payroll billing codes for the IT Manager and Junior IT Specialist at the *FFPLTC*
- Establish payroll billing codes for the IT Coordinator at the Civic Centre
- Establish expanded responsibility scope compensation in the case of prolonged absences

A2) Equipment

- Provision a mobile phone for the IT Coordinator, allocated as a monthly *ToFF* expense
- Provision a laptop for the IT Coordinator, attached to the *ToFF* domain
- Develop a process by which emergency purchasing can be achieved when required, given the approval of the *ToFF* CAO in the absence of the IT Manager

A3) Access

- Define the scope and duration of building access for each employee
    - Produce keys, fobs and codes where required
- Implement scoped service accounts and role-based access control for each system
- Define the scope and duration of system access for each employee
    - Determine whether this access is always-on or toggled off when not required

A4) Scheduling

- Deploy incident response and networking monitoring software to the IT Coordinator and Junior IT Specialist
- Develop incident duration and call-in tracking procedures
- Develop a work-alone procedure that informs the chain of command when responding to critical incidents

A5) Documentation

- Develop a list of critical and non-critical systems
    - Survey department heads
    - Determine what systems will be addressed outside of regularly scheduled work hours
- Develop incident response plans for each system
- Develop reference documentation for each facility
- Develop network maps
- Enable robust domain logging and test output
- Update in Active Directory:
    - Active computer and user lists
    - Security groups for software deployments and network resource access

A6) Support

- Implement a CRM ticketing solution common to both the *ToFF* and *FFPLTC*
- Delegate access to the support@fortfrances.ca shared mailbox to the IT Coordinator
- Educate staff about support request procedures

A7) Training

- Complete heights training for each employee
- Schedule the IT Coordinator to be present at the Civic Centre for 1 morning of training each week until the IT Manager is satisfied with the operational capacity achieved
- Schedule the Junior IT Specialist to be present at the *FFPLTC* for 1 morning of training each week until the IT Coordinator and IT Manager are mutually satisfied with the operational capacity achieved
- Schedule training as required for each site and employee, whenever *ToFF* or *FFPLTC* infrastructure changes take place
- Include site visits to each *ToFF* facility in training sessions

A8) Approval

- Changes to the support relationship between the *ToFF* and *FFPLTC* will require mutual agreement between both parties

A9) Implications of Access

- By engaging additional employees with greater access to IT systems, there is an increased scope of liability for the *ToFF*. Employees may gain access to resources, such as: financial software, payroll, human resources data, etc. A policy detailing the interaction with these datasets and privileges may be required to ensure confidentiality and responsibility. These privileges may be mitigated through more granular access schemes, but this will limit the ability of employees to respond to incidents.
- Additional users of network monitoring utilities will require additional software licenses, resulting in additional operating expenditures.
- Additional users may have to be added to external support services lists to facilitate access to third-party support services.

A10) Future Considerations

- Potential integration of *ToFF* and *FFPLTC* domains
- Potential integration of networks
- Potential homogenization of systems
- Conversely, the potential isolation of networks, email, and telephone services

A10.1) Research

- Continue building network contacts with other municipalities
- Continue researching how other organizations approach IT coverage