Dunn Companies IT (DCIT) Priorities & Policies

15 December 2025

Dunn Companies IT Strategy:
Support Dunn Companies to improve profitability through efficiency, risk reduction, regulation compliance with a bias for action centered in progressive technology advancement to develop a culture of security

Priorities (in order)

- Security: Infrastructure Integrity and Connectivity
- Legal: Adherence to all applicable regulations, laws, guidance, etc
- Customer Facing / Revenue Generating
- Payroll & Accounts Payable
- Maintenance
- Help Desk: Ranges from individual user issues to third-party software patches
- On-Boarding: OpCo HR should notify IT 5 business days prior to needed activation
- Training
- Innovation
- Special Projects: DIC Acquisitions & Divestitures will be prioritized by specific need

Work Order Process – How to Request Support

Primary Method – DunnSupport.com
Enter a Support Ticket: Complete form to generate work order

Secondary Method – Automate Agent in System Tray
Right-click icon and “Create Service Ticket”

If unable to utilize DunnSupport.com, call DCIT Hotline: 833-626-0379

Emergencies to include stop-work plant down, employee termination, suspicious email or Real-world IT Incident
DCIT Hotline 833-626-0379
Press 1 - Emergency condition, call will be routed to on-call DCIT
(6AM CST – 7PM CST)
Press 2 – Non-emergency Support Requests
(7AM CST – 4PM CST)

Tickets regarding Command Batch PC’s or Jonel Machines will be handled by Kyle Beckman / Mark Burks Team. Tickets can be placed through the same methods but will be forwarded to the appropriate team for resolution.

DunnSupport.com *Note that not all items are available to all users*

MAIN PAGE OPTIONS

Enter a Support Ticket
This allows you to enter tickets as well as track all your tickets/requests.

Feedback
Utilize this to provide feedback on individual/issue.

PORTAL OPTIONS – SUBMIT NEW TICKET

Enter a Support Ticket
Complete form to generate work order.
All IT efforts must originate with submitted ticket.

Hardware Request
Use this form to request new hardware.
"Approved By" block must contain proper level of OpCo approval to purchase the requested equipment. Approval will not be confirmed by DCIT team.

New Employee
HR Only
Please complete 5 working days before need.
Once this ticket is submitted, DCIT team will verify with requestor prior to establishing new service with appropriate rights. This will serve as two-factor authentication.

Employee Role Change
HR Only
Request new access to system resources for existing employees.

Employee Termination
HR Only
Off-Boarding - for non-time critical or contact DCIT Hotline Option 1 for time critical situations.

Email Release
Request emails to be released from quarantine.

International Travel Request access to system resources while traveling. *HR Only*

IT response guarantees:

- All emergency tickets will receive immediate priority.
- All other priority tickets will be acknowledged within 60 minutes during normal operating hours and addressed promptly.
- All emails to Dunn Companies IT members will be acknowledged <24 hours to sender.

Thanks to everyone for the teamwork as we continue to innovate and adapt our system to best serve each of you, the customers of Dunn Companies IT. This effort aligns with the direction of our statement of values to deeply value excellence and continuous improvement.

Computer Update, Patching & Restart Policy

Domain computers only (CommandBatch & Apex PCs excluded from updates under this policy)

- Patching will occur every Thursday night at 9 PM
- Users will receive a message earlier in the day reminding them of what will happen at 9PM
- When finished for the day, users will close out of all programs, log out, and leave their PC powered ON (preference is restart computer as you leave)
- Computers will automatically be restarted after patching has completed
- Optional - We give any users logged in and actively using the computer at 9 PM (i.e. CommandSeries plant PCs) the option to delay the restart once for a specified time
- NOTE: DRB is on Wednesday nights, controlled by Burton's

Dunn Companies IT Security Training Policy

Dunn continues to partner with Arctic Wolf to provide monthly comprehensive security training for all employees to better protect our organization from external threats. Each month every user will receive at least one short training video that will cover an aspect of cyber security in today's world. Arctic Wolf also provides simulated phishing emails to test user's security awareness, and failure of a simulated phishing attack also automatically assigns a related security training module. It is imperative that all employees receiving these training videos complete the training in a timely manner.

The participation of all employees involved in the training program will be reviewed at the beginning of each month. Any employee with 2 incomplete training modules over 30 days old will have their account locked. Once an employee's account has been locked due to non-compliance, the affected employee must speak with their supervisor to submit a request to have the account unlocked via DunnSupport.com. Note that requests to unlock accounts submitted after hours will be handled the next business day. Once a user's account has been unlocked, a follow-up email will be sent including links to their missing training videos. If these videos are not completed within one business day the account will be locked again and the subsequent unlock request must be received from the Operating Company President.

Password Requirements

Dunn Passwords must be a minimum of 12 characters to include 3 of these 4-character types: Upper Case, Lower Case, Number, Special Character. Passwords must not include Username, First or Last name. Passwords should not include easily identifiable information like wedding or birthdates. All passwords will be reset every 180 days.

International Travel

- Employees who are traveling internationally and desire to access company email or files must submit an international travel request through their respective HR professional prior to travel dates.
- HR personnel will submit international travel ticket (option is not available to anyone outside of HR) with country and start/stop dates.
  - Note that contacting IT staff directly will not result in access being granted. Internal access can only be granted via the approval path through HR.
- IT Staff will follow the internal approval procedure once request is entered by HR.
- Countries of access approval will be weighed with the threat rating of the country and the risk we choose to accept.

Usernames

Dunn Companies IT requires each user to have a unique username with no shared log-ins. Any user found to be sharing their password or using another member's password will result in both members being locked out of our system immediately with minimum of OpCo VP request to CTO for reactivation.

Real-world IT Security Incident

A real-world IT Incident is defined as any action by a member that jeopardizes the security or integrity of our IT infrastructure. This ranges from clicking a nefarious link to downloading software or attachments that could yield a breach of our security. Incidents will be handled uniquely to the actions and impact to our system at the OpCo President level with immediate suspension of the account until the investigation and remediation actions have been completed.

Consent to Monitoring

Company IT assets may be monitored, inspected, and/or searched at any time. No expectation of privacy should be inferred or assumed on any IT asset owned and/or provided by the company to the employee. Personal data that the employee does not want to be subject to potential monitoring should not be kept on corporate assets. No attempt should be made to bypass monitoring by the employee, including (but not limited to) the use of personal email or online services to transfer corporate data, or installing any software intended to be used to bypass monitoring of data security.

FortiMail/Abnormal Security

FortiMail and Abnormal Security are two of several layers of security protection in use to monitor email and data security (both incoming and outgoing data). The presence of technology monitoring data security does not eliminate the need for the users to use due diligence and critical thinking in securing company data but is there as an extra layer of protection against possible mistakes or "day one" vulnerabilities that are otherwise unknown to both the users and the DCIT staff.

Artificial Intelligence (AI)

Internal AI is not currently allowed on company servers or networks. Any desire to utilize an AI capability on our network should be brought to the attention of DCIT before any contracts are signed. The issue is confidentiality. Employees, contractors, vendors, and other users of Dunn Companies systems must not input, upload, or disclose any confidential, proprietary, regulated, or otherwise sensitive information into AI services such as ChatGPT, Google Gemini, or Claude. At this time, no AI will be allowed on the DCIT enterprise servers.

New Software

Any new software to be installed on company computers should be approved by DCIT before purchase to ensure compatibility with our IT enterprise.

Server Reboot

Servers will be selectively rebooted on Sundays 12am-5am. Please notify DCIT in advance if any company work must be accomplished during those times.

Instructions to OpCo HR Lead

This “Priorities & Policies” should be acknowledged by every user prior to activation of their account. This could be from inclusion in OpCo employee handbook or separate signature to be maintained in HR file.