Back-to-School Check List

Back to school is a stressful time for publishers, colleges and universities, school districts, EdTech firms, and their vendors and partners. Based on our 30+ years of experience helping customers through this challenging time period, Unicon has compiled a collection of practices and preparations that you can put in place to help ensure a smooth back-to-school experience. Contact us if you would like to learn more or need help evaluating your readiness.

People

- □ Ensure that coverage areas are clear, including who has primary or secondary responsibility for all applications and infrastructure (responsibility matrix).
- □ Make sure that staffing plans are communicated - if anyone is out or unavailable, ensure that the backup personnel are identified, prepared, and have been communicated with.

Processes

- □ Are incident handling processes well defined and do the various teams and people understand their roles? Be sure that lines of communication (email, phone, incident conference call numbers) between support, technology, product, and sales are clear and roles are clear. Hold a refresher session if needed. Make sure escalation plans are also clear (when other people and teams are called in).
- □ Will change management and/or deployment processes be different during back to school - e.g. a change "freeze" or extra scrutiny if pushing bug fixes or other critical patches? Who will review the associated risks and approve the changes?
- □ Make sure incident and change processes include critical vendors/partners.
- □ Confirm that run books and other process documentation are up to date.

Product and Application

- □ Have release plans been communicated to customers? If there are planned outages for deployment, maintenance, new year roll-over, or other, make sure those are communicated to customers with sufficient advance notice as well as reminders in the days before the outage.
- □ Is product training and documentation released and available for both clients and internal staff?
- □ If there are work-arounds for bugs or other known issues, make sure that support staff, knowledge base/self-help assets, and proactive training or communications are available.

- □ Have all quality activities been completed, including functional tests, regression tests, integration tests, performance tests, application security tests, and others as needed? Have the results been communicated to support, sales and other stakeholders and any remaining risks addressed or accepted, and action items (work-arounds, patch release plans, etc.) been completed or are on track?
- □ Has new content been fully deployed and tested, factoring in CDNs and/or other content caching/delivery?

Infrastructure

- □ Capacity plan - has the projected load been estimated and plans put in place to meet the load and been verified? This could be statically deployed resources or dynamic "autoscale" resources. If dynamic, the scaling mechanisms should be tested and appropriate cost monitoring in place. Be sure to include all tiers of the infrastructure - networking, compute, storage (both structured and unstructured, e.g. database, object stores, file systems), integration and messaging components, caching, CDN, IAM, etc. If manual activities are needed to scale, ensure that the deployment processes are well defined and tested.
- □ Monitoring and alerting should be reviewed and tested to ensure that the right people are notified to respond to application or component issues. Self-healing should be tested.
- □ Disaster recovery, data recovery, and/or backup and restore procedures should be tested and verified as current, ensuring that all staff know their roles and responsibilities.

Security

- □ Are security incident response processes well defined and roles and responsibilities documented and well understood? Consider a refresher or table top exercise.
- □ Have security patches been deployed and verified, both for infrastructure, tech stack, and applications?
- □ Has security monitoring such as intrusion detection/prevention, security event monitoring, and alerting been tested and is it working as designed?
- □ Consider suspending potentially disruptive activities such as vulnerability scanning and/or penetration testing during the back-to-school period.

UNICON®

1447 W Elliot Road, Suite 101
Gilbert, AZ 85233
480.558.2400 Phone
info@unicon.net
www.unicon.net