OXFORD
COLLEGE OF MANAGEMENT

HR Cybersecurity Robustness Checklist

Data Classification and Handling

- [ ] Classify Data: Identify and classify data based on sensitivity and confidentiality requirements.
- [ ] Access Controls: Implement strict access controls and permissions for sensitive data.

Employee Onboarding and Offboarding

- [ ] Security Training: Include cybersecurity awareness training as part of the onboarding process.
- [ ] Account Management: Ensure proper procedures for deactivating access rights and returning company assets during offboarding.

Regular Cybersecurity Training

- [ ] Ongoing Education: Conduct regular cybersecurity training sessions and updates.
- [ ] Phishing Simulations: Regularly test employees with mock phishing scenarios to enhance vigilance.

Policy Development and Enforcement

- [ ] Clear Policies: Develop clear cybersecurity policies covering aspects like acceptable use, data protection, and mobile device management.
- [ ] Policy Reviews: Regularly review and update policies to adapt to new cybersecurity threats and changes in technology.

Incident Response Planning

- [ ] Response Team: Establish a dedicated incident response team with clear roles and responsibilities.
- [ ] Action Plan: Develop and maintain an incident response plan that includes notification procedures and steps for containment and recovery.

Vendor Management

- [ ] Vendor Assessments: Assess the security measures of all vendors who handle sensitive information.
- [ ] Contracts and Agreements: Include cybersecurity requirements and obligations in contracts with third parties.

Compliance and Legal Requirements

- [ ] Regulatory Compliance: Ensure all practices comply with relevant laws and regulations such as GDPR.
- [ ] Legal Consultations: Regularly consult with legal professionals to address compliance and regulatory changes.

Technology and Security Tools

- [ ] Secure Platforms: Use secure platforms for data storage and communication.
- [ ] Multi-Factor Authentication (MFA): Implement MFA for accessing critical systems and information.

Remote Work Security

- [ ] Secure Connections: Ensure that remote connections are secured via VPNs or other secure methods.
- [ ] Device Security: Implement security measures for personal and company devices used in remote work.

Regular Audits and Assessments

- [ ] Security Audits: Conduct regular security audits to identify vulnerabilities.
- [ ] Risk Assessments: Perform thorough risk assessments to understand and mitigate potential threats.

Monitoring and Reporting

- [ ] Monitoring Systems: Implement systems to monitor and log access to sensitive data.
- [ ] Breach Notification: Establish a protocol for timely reporting of any security incidents or breaches.

This checklist is designed to be comprehensive but should be adapted to the specific needs and context of your organisation. Regular reviews and updates to this checklist will help maintain its relevance as technologies and threat landscapes evolve.