يتم تطوير أنظمة الذكاء الاصطناعي لتكون محمية بطريقة آمنة وتراعي المتطلبات النظامية ذات العلاقة، ومن ذلك المتطلبات النظامية المتعلقة بحماية خصوصية أصحاب البيانات الشخصية، بهدف منع الوصول غير المشروع إلى البيانات والنظام مما قد يؤدي إلى الإضرار ويتم تصميم أنظمة الذكاء الاصطناعي باستخدام آليات وضوابط توفر إمكانية إدارة ومراقبة النتائج والتقدم الذي يتم طوال دورتها لضمان امتثالها بقواعد وضوابط الخصوصية والأمن ذات العلاقة